PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-349725

(43)Date of publication of application : 15.12.2000

(51)Int.Cl. H04H 1/00
H04B 1/16
H04L 9/08
H04L 9/36
H04N 5/44
H04N 7/16

(21)Application number : 11-158212

(22)Date of filing : 04.06.1999

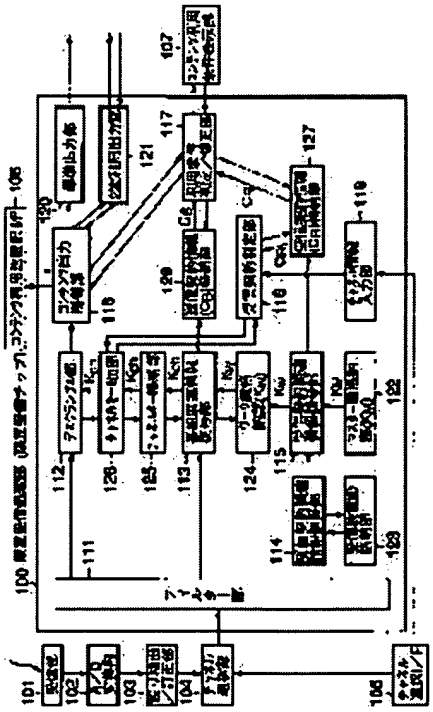
(71)Applicant : TOSHIBA CORP

(72)Inventor : AKIYAMA KOICHIRO

(54) BROADCAST RECEPTION DEVICE AND CONTENT USE CONTROL METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To control use of every content by synthesizing first use condition information common to a plurality of pieces of content information and second use condition information which is broadcast in accordance with the plurality of pieces of content information and is common to a plurality of contractors, deciding a use condition on designated content information and controlling the use of corresponding content information.



SOLUTION: Priority is given to individual conditions and an order is given to unified content use conditions in accordance with the priority and the contract use condition of the highest priority is set to be a corrected use condition. Since first priority is given to the limit of the number of items, a use possible contract information list is referred to from the limit of the number of times. When use possible contract information satisfying the condition does not exist, the use possible contract information list having the largest number of designation of limit information on the number of times is extracted and the list is similarly generated. The contract condition whose period is the longest is extracted and the corrected content use condition is generated.

THIS PAGE BLANK (USPTO)

LEGAL STATUS

[Date of request for examination]	12.09.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3695992
[Date of registration]	08.07.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）

(11)特許出願公開番号
特開2000－349725
（Ｐ２０００－３４９７２５Ａ）
(43)公開日　平成12年12月15日(2000.12.15)

(51)Int.Cl.[7]	識別記号	F.I		テーマコード（参考）
H04H 1/00		H04H 1/00		F 5C025
H04B 1/16		H04B 1/16		G 5C064
H04L 9/08		H04N 5/44		D 5J104
9/36		7/16		Z 5K061
H04N 5/44		H04L 9/00	601	A

審査請求　未請求　請求項の数13　ＯＬ　（全38頁）　最終頁に続く

(21)出願番号　特願平11－158212

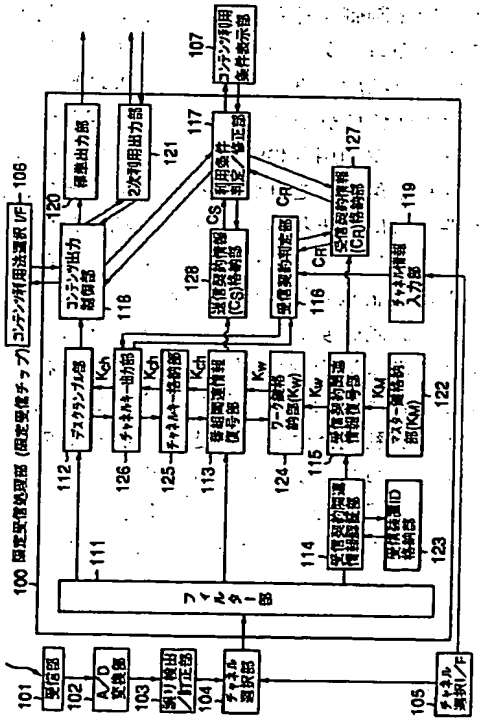
(22)出願日　平成11年６月４日(1999.6.4)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　秋山　浩一郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】放送受信装置及びコンテンツ利用制御方法

(57)【要約】
【課題】　放送コンテンツに応じて２次利用を制御可能な放送受信装置を提供すること。
【解決手段】　放送配信されるコンテンツ情報の利用を利用条件に応じて制御する放送受信装置であって、個々の契約者に対応して放送される、同じチャネルに含まれる複数のコンテンツ情報に共通の、チャネル受信契約情報と、個々のコンテンツ情報に対応して放送される、複数の契約者に共通の、チャネル送信契約情報とを統合して、指定されたコンテンツ情報に対応する利用可能契約情報リストを作成し、作成された利用可能契約情報リストに基づいて、コンテンツ利用条件を決定し、決定されたコンテンツ利用条件に基づいて、受信されたコンテンツ情報の利用を制御する。



1

【特許請求の範囲】

【請求項１】チャネルを用いて放送配信されるコンテンツ情報を受信する手段と、

複数のコンテンツ情報を含むチャネルに対応して放送された、個々の契約者に対する第１の利用条件情報と、個々のコンテンツ情報に対応して放送された、複数の契約者に共通の第２の利用条件情報とを統合して、指定されたコンテンツ情報に対応する第３の利用条件情報を作成する手段と、

作成された前記第３の利用条件情報に基づいて決定されたコンテンツ利用条件に従って、受信された対応する前記コンテンツ情報の利用を制御する手段とを備えたことを特徴とする放送受信装置。

【請求項２】前記制御する手段は、決定された前記コンテンツ利用条件に基づいてコンテンツ情報の２次利用に対する制御を行う手段を含むことを特徴とする請求項１に記載の放送受信装置。

【請求項３】前記制御する手段は、

前記コンテンツ情報を２次利用する２次利用装置がその利用制御の際に従うべき条件を規定したライセンス情報を、決定された前記コンテンツ利用条件に基づいて作成する手段と、

前記コンテンツ情報を暗号化する手段と、

暗号化された前記コンテンツ情報を復号するための鍵と、前記ライセンス情報とを一体化して暗号化する手段と、

暗号化された前記コンテンツ情報と、暗号化された前記鍵および前記ライセンス情報とを、前記２次利用装置に送信する手段と含むことを特徴とする請求項１に記載の放送受信装置。

【請求項４】前記制御する手段は、前記第３の利用条件情報として複数のコンテンツ利用条件が作成された場合に、各コンテンツ利用条件に含まれる制限項目毎に予め定められた優先順位に従って、該第３の利用条件情報に含まれるコンテンツ利用条件と、入力されたユーザ所望のコンテンツ利用条件とを比較することによって、該第３の利用条件情報に含まれるコンテンツ利用条件を１つに定める手段を含むことを特徴とする請求項１ないし３のいずれか１項に記載の放送受信装置。

【請求項５】前記制御する手段は、前記第３の利用条件情報として複数のコンテンツ利用条件が作成された場合に、予め定められた評価関数に従い、入力されたユーザ所望のコンテンツ利用条件を基準とし、該第３の利用条件情報に含まれるコンテンツ利用条件の各々を評価することによって、該第３の利用条件情報に含まれるコンテンツ利用条件を１つに定める手段を含むことを特徴とする請求項１ないし３のいずれか１項に記載の放送受信装置。

【請求項６】前記制御する手段は、前記第３の利用条件情報として複数のコンテンツ利用条件が作成された場合

2

に、該複数のコンテンツ利用条件を提示し、ユーザからの選択指定を受け付けることにより、該第３の利用条件情報に含まれるコンテンツ利用条件を１つに定める手段を含むことを特徴とする請求項１ないし３のいずれか１項に記載の放送受信装置。

【請求項７】前記制御する手段は、前記第３の利用条件情報に含まれるコンテンツ利用条件のうちに、入力されたユーザ所望のコンテンツ利用条件を包含するものが存在する場合には、該ユーザ所望のコンテンツ利用条件を採用することを決定し、該ユーザ所望のコンテンツ利用条件を包含するものが存在しない場合には、該ユーザ所望のコンテンツ利用条件を該前記第３の利用条件情報に適合するように修正したものを採用することを決定することを特徴とする請求項１ないし６のいずれか１項にに記載の放送受信装置。

【請求項８】前記コンテンツ利用条件の利用制限項目として、有効期限に関する条件、利用回数に関する条件、および機器または機種の限定に関する条件の少なくとも１つを含むことを特徴とする請求項１ないし７のいずれか１項に記載の放送受信装置。

【請求項９】前記制御する手段は、前記コンテンツ情報を２次利用装置に送信する場合に、該２次利用装置に対する認証を行なう手段を含むことを特徴とする請求項１ないし放送受信装置。

【請求項１０】前記第２の利用条件情報は、対応するコンテンツ情報と同一のパケットに含まれて放送されることを特徴とする請求項１ないし９に記載の放送受信装置。

【請求項１１】前記第２の利用条件情報は、対応するコンテンツ情報に対する電子番組ガイド情報と同一のパケットに含まれて放送されることを特徴とする請求項１ないし９に記載の放送受信装置。

【請求項１２】前記制御する手段によるコンテンツ利用条件の決定を、録画予約時に行うことを特徴とする請求項１１に記載の放送受信装置。

【請求項１３】放送配信されるコンテンツ情報の利用を利用条件に応じて制御するコンテンツ利用制御方法であって、個々の契約者に対応して放送される、同じチャネルに含まれる複数のコンテンツ情報に共通の、第１の利用条件情報と、個々のコンテンツ情報に対応して放送される、複数の契約者に共通の、第２の利用条件情報とを統合して、指定されたコンテンツ情報に対する利用条件を定め、定められた前記利用条件に基づいて、対応する前記コンテンツ情報の利用を制御することを特徴とするコンテンツ利用制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化（スクランブル）されて放送配信されるコンテンツを契約内容（例えば、期間、視聴チャネル、録画録音の可否）に応じて

復号（デスクランブル）し利用あるいは２次利用する有料放送サービスのための契約受信装置及びコンテンツ利用制御方法に関する。

【０００２】

【従来の技術】デジタル放送は、通信衛星（ＣＳ）に始まって、ケーブルＴＶ、地上放送へとデジタル化が進むにつれ、一層のサービスの充実が期待されており、これからに放送サービスの主役を務めていくものと思われる。

【０００３】デジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャネル数の大幅な増加が可能となったことである。さらに、高度な誤り訂正技術が適用できるため、高品質で均質なサービスの提供が可能となる。

【０００４】また、放送のデジタル化により、従来のように画像や音声による放送だけでなく、文字やデータによる放送（データ放送）も可能になり、例えばニュースを文字データとして流すことや、ＰＣソフトを放送で配信することが可能となり、そのようなサービスを提供するためのシステムも続々と登場してきている。

【０００５】このようなシステムで、契約内容に基づいてスクランブルを解く、あるいは復号する有料放送サービスを提供する際、契約期間に即した顧客管理が行えなければならない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャネルの番組の視聴を可能とするというものである。

【０００６】また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する上からも正当な視聴者のみに（契約チャネル、契約期間に即して）しかも確実に提供する必要がある。

【０００７】この意味で、従来は、図５に示すような鍵構成を用いて限定受信を行なっていた。すなわち、放送受信装置毎にマスター鍵K_Mを用意し、受信契約している視聴者に対して受信契約しているチャネルのワーク鍵K_wと受信契約情報をマスター鍵K_Mで暗号化して送信する。ここで、ワーク鍵はチャネル固有の鍵であり、受信契約情報は当該チャネルの契約期間あるいは契約の有無などの情報である。受信契約情報は、コンテンツ受信に先だって受信し、蓄積される。コンテンツ視聴時は、当該受信契約に関する情報を参照して、当該チャネルの視聴可否によって、ワーク鍵を使って暗号化されて送られてくる当該チャネルのチャネルキーK_{ch}を復号して視聴する。チャネルキーは、スクランブルされた放送コンテンツをデスクランブルするのに用いられる。

【０００８】このように従来のデジタル放送方式では、有料放送を実現する手段として受信契約情報を用いていた。これによって、チャネル毎の契約管理を確実に行うことができ、デジタル放送が事業として成立している。しかしながら、チャネル毎の受信契約しかサポートできず、同一チャネル内に存在するコンテンツの価値などにまで踏み込んだ視聴管理は不可能であった。これは、例えば、２次利用を前提としたＰＣソフトなどのデータ放送や、高付加価値な映画コンテンツの録画の際には、録画可否をチャネル単位でしか指定できないため問題が多かった。

【０００９】

【発明が解決しようとする課題】以上のように、従来の限定受信システムでは、コンテンツ毎の利用制御が困難であった。

【００１０】本発明は、上記事情を考慮してなされたもので、コンテンツ毎の利用制御を可能とする放送受信装置及びコンテンツ利用制御方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は、放送配信されるコンテンツ情報の利用を利用条件に応じて制御するコンテンツ利用制御方法であって、個々の契約者に対応して放送される、同じチャネルに含まれる複数のコンテンツ情報に共通の、第１の利用条件情報と、個々のコンテンツ情報に対応して放送される、複数の契約者に共通の、第２の利用条件情報とを統合して、指定されたコンテンツ情報に対する利用条件を定め、定められた前記利用条件に基づいて、対応する前記コンテンツ情報の利用を制御することを特徴とする。

【００１２】本発明（請求項１）は、チャネルを用いて放送配信されるコンテンツ情報を受信する手段と、複数のコンテンツ情報を含むチャネルに対応して放送された、個々の契約者に対する第１の利用条件情報（例えば、チャネル受信契約情報に含まれる１または複数のコンテンツ利用情報）と、個々のコンテンツ情報に対応して放送された、複数の契約者に共通の第２の利用条件情報（例えば、チャネル送信契約情報に含まれる１または複数のコンテンツ利用情報）とを統合して、指定されたコンテンツ情報に対応する第３の利用条件情報（例えば、利用可能契約情報リスト）を作成する手段と、作成された前記第３の利用条件情報に基づいて決定されたコンテンツ利用条件に従って、受信された対応する前記コンテンツ情報の利用を制御する手段とを備えたことを特徴とする。

【００１３】好ましくは、前記制御する手段は、決定された前記コンテンツ利用条件に基づいてコンテンツ情報の２次利用に対する制御を行う手段を含むようにしてもよい。

【００１４】好ましくは、前記制御する手段は、前記コンテンツ情報を２次利用する２次利用装置がその利用制御の際に従うべき条件を規定したライセンス情報を、決定された前記コンテンツ利用条件に基づいて作成する手段と、前記コンテンツ情報を暗号化する手段と、暗号化

された前記コンテンツ情報を復号するための鍵と、前記ライセンス情報とを一体化して暗号化する手段と、暗号化された前記コンテンツ情報と、暗号化された前記鍵および前記ライセンス情報とを、前記２次利用装置に送信する手段と含むようにしてもよい。このようにコンテンツ情報とリンクしたライセンス情報を作成することによって、コンテンツの２次利用における利用制御を可能とする。

【００１５】好ましくは、前記制御する手段は、前記第３の利用条件情報として複数のコンテンツ利用条件が作成された場合に、各コンテンツ利用条件に含まれる制限項目毎に予め定められた優先順位に従って、該第３の利用条件情報に含まれるコンテンツ利用条件と、入力されたユーザ所望のコンテンツ利用条件とを比較することによって、該第３の利用条件情報に含まれるコンテンツ利用条件を１つに定める手段を含むようにしてもよい。

【００１６】好ましくは、前記制御する手段は、前記第３の利用条件情報として複数のコンテンツ利用条件が作成された場合に、予め定められた評価関数に従い、入力されたユーザ所望のコンテンツ利用条件を基準とし、該第３の利用条件情報に含まれるコンテンツ利用条件の各々を評価することによって、該第３の利用条件情報に含まれるコンテンツ利用条件を１つに定める手段を含むようにしてもよい。この場合に、好ましくは、前記第３の利用条件情報として複数のコンテンツ利用条件が作成された場合に、予め定められた評価関数による評価値に基づいた順番で該複数のコンテンツ利用条件を表示し、ユーザに選択などをさせるようにしてもよい。

【００１７】好ましくは、前記制御する手段は、前記第３の利用条件情報として複数のコンテンツ利用条件が作成された場合に、該複数のコンテンツ利用条件を提示し、ユーザからの選択指定を受け付けることにより、該第３の利用条件情報に含まれるコンテンツ利用条件を１つに定める手段を含むようにしてもよい。

【００１８】好ましくは、前記制御する手段は、前記第３の利用条件情報に含まれるコンテンツ利用条件のうちに、入力されたユーザ所望のコンテンツ利用条件を包含するものが存在する場合には、該ユーザ所望のコンテンツ利用条件を採用することを決定し、該ユーザ所望のコンテンツ利用条件を包含するものが存在しない場合には、該ユーザ所望のコンテンツ利用条件を該前記第３の利用条件情報に適合するように修正したものを採用することを決定するようにしてもよい。

【００１９】好ましくは、決定されたコンテンツ利用条件を表示してユーザに通知するようにしてもよい。

【００２０】好ましくは、前記コンテンツ利用条件の利用制限項目として、有効期限に関する条件、利用回数に関する条件、および機器または機種の限定に関する条件の少なくとも１つを含むようにしてもよい。

【００２１】好ましくは、前記制御する手段は、前記コンテンツ情報を２次利用装置に送信する場合に、該２次利用装置に対する認証を行なう手段を含むようにしてもよい。あるいは、放送受信装置と２次利用装置との間で相互認証を行なうようにしてもよい。

【００２２】好ましくは、前記第２の利用条件情報は、対応するコンテンツ情報と同一のパケットに含まれて放送されるようにしてもよい。

【００２３】好ましくは、前記第２の利用条件情報は、対応するコンテンツ情報に対する電子番組ガイド情報と同一のパケットに含まれて放送されるようにしてもよい。

【００２４】好ましくは、前記制御する手段によるコンテンツ利用条件の決定を、録画予約時に行うようにしてもよい。

【００２５】本発明（請求項１３）は、放送配信されるコンテンツ情報の利用を利用条件に応じて制御するコンテンツ利用制御方法であって、個々の契約者に対応して放送される、同じチャネルに含まれる複数のコンテンツ情報に共通の、第１の利用条件情報と、個々のコンテンツ情報に対応して放送される、複数の契約者に共通の、第２の利用条件情報とを統合して、指定されたコンテンツ情報に対する利用条件を定め、定められた前記利用条件に基づいて、対応する前記コンテンツ情報の利用を制御することを特徴とする。

【００２６】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００２７】本発明によれば、あるチャネルに対して契約者が持っている１または複数の第１の利用条件と、あるコンテンツに対して規定されている１または複数の第２の利用条件とを統合することによって、契約者とコンテンツのペア毎に様々な限定受信を実現することができる。このことにより、コンテンツの価値などに応じてコンテンツ毎に利用制御することが可能になり、また、従来は十分にできていなかったコンテンツの２次利用などへも限定受信を拡張することができる。

【００２８】また、コンテンツ利用条件をライセンス情報という形でコンテンツとリンクさせて２次利用装置に与えることによって、コンテンツを２次利用装置に利用させることが可能になる。

【００２９】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００３０】最初に、基本的事項の説明や語句の定義等を行なう。

【００３１】放送受信装置のコントロールが直接的には及ばない機器・装置（２次利用装置と呼ぶ）でのコンテンツの利用を「２次利用」と呼ぶ。２次利用以外のコンテンツの利用を「標準利用」と呼ぶ。例えば、録画装置やＰＣ等の外部装置は２次利用の制御の対象になるが、

放送受信装置と一体化されて放送受信装置のコントロールが直接及ぶテレビ出力装置やスピーカのような機器・装置（標準利用装置と呼ぶ）は２次利用の制御の対象にはなない（もちろん、同種のテレビ出力装置やスピーカであっても放送受信装置のコントロールが直接的には及ばなければ２次利用装置になる）。

【００３２】本実施形態では、放送受信装置が行う限定受信として、標準利用装置に関する制御（例えば、放送中のコンテンツの即時的な視聴の可否に対するチャネル受信契約に基づく制御）と、２次利用装置での適正なコンテンツの利用を可能にするための制御を例として取り上げている。

【００３３】本実施形態では、個々のユーザが番組提供側（例えば放送局）との間で基本的にはチャネル単位で受信契約する場合を想定している。また、基本的にはユーザ毎かつチャネル毎に契約内容（例えば利用条件）が設定される場合を想定している。少なくとも１つのチャネルの受信契約をしたユーザ側には、限定受信を行う放送受信装置が設置される。各放送受信装置には固有の識別子（受信装置ＩＤと呼ぶ）が付され、放送受信装置はこの「受信装置ＩＤ」により管理される。

【００３４】或るチャネルの契約状態（例えば、契約の有無、利用条件など）を示す情報を「チャネル契約情報」と呼ぶ。チャネル契約情報は、限定受信を行なうために放送局側から放送受信装置側に放送される制御情報である（適正な放送受信装置は、制御情報に従って限定受信のための制御を行う）。本実施形態では、本来のチャネル受信契約によって設定される（コンテンツ依存性のない）「チャネル受信契約情報」と、コンテンツの価値や個性などに応じて送信側の意図によって設定される（コンテンツ依存性のある）「チャネル送信契約情報」の２種類のチャネル契約情報を用いる。チャネル受信契約情報は、例えば、契約者毎かつチャネル毎に設定され（１つのチャネルに含まれるコンテンツに共通に設定され）、チャネル送信契約情報は、例えば、チャネル毎かつコンテンツ毎に設定される（契約者に共通に設定される）。

【００３５】ところで、契約状態を契約の有無のみとして考えた場合、例えば、各チャネルにチャネル番号を付け、図２のようにチャネル番号に対応したビットが１であるか否かによりチャネルの契約の有無を表したビット列が、チャネル契約情報の一形態である。このように各チャネル毎にその契約の有無を表記した情報をチャネル展開情報と呼ぶ。全チャネルでｎチャネルあるならば、チャネル展開情報はｎビットのデータとなる。図２の例では、全８チャネルのうち、第２、第５、第７、第８チャネルが契約済であり、第１、第３、第４、第６チャネルが未契約であることを示している。

【００３６】ここで、特定のチャネルに対応する、そのチャネルの契約状態を示すビット情報を「契約フラグ」と呼ぶ。例えば、図２のチャネル契約情報においては、第１チャネルの契約フラグは０、第２チャネルの契約フラグは１である。

【００３７】放送受信装置内において記憶されている契約フラグは、対応するチャネルの契約の有無を表すことになるが、放送局から放送する情報の中に含める契約フラグは、対応するチャネルが新規契約されたこと（放送受信装置内において記憶されている契約フラグを０から１へ更新させる場合）、対応するチャネルの契約が解除されたこと（放送受信装置内において記憶されている契約フラグを１から０へ更新させる場合）、対応するチャネルの契約の有無の確認（契約フラグが変化しない場合）などを通知するために使用できる。

【００３８】チャネルおよび契約フラグの通知（放送）の方法には、上記のチャネル展開情報を用いる方法の他に、種々の方法がある。例えば、図３のように、チャネル識別子とその契約フラグの組を用いて、チャネル契約情報を個別に通知する方法がある。この場合には、必要なチャネル（例えば、新規契約されたチャネル、契約解除されたチャネル、確認等のために契約状態を通知するチャネル等）についてだけ放送するようにすることができる。また、図３において、チャネル識別子を複数列挙して、複数のチャネルの契約状態を取り纏めて通知する方法もある。あるいは、複数のチャネル識別子の組を示すパッケージ識別子を用いて、複数のチャネルの契約状態を取り纏めて通知する（あるパッケージ識別子に含まれる複数のチャネル識別子の組を示す情報は別途放送する）方法もある。本発明はどのような形態にも適用可能であるが、本実施形態では図３に示す方法を用いる場合を例にとって説明する。

【００３９】また、本実施形態では、契約状態として、チャネル毎の契約の有無だけではなく、より高度な限定受信の実現のために、チャネルに関する契約内容（例えば利用条件）およびコンテンツに関する契約内容（例えば利用条件）を用いる。このために、チャネル受信契約情報／チャネル送信契約情報には、契約フラグの他に、契約内容に関する情報、例えば図４に示すコンテンツ利用情報が含まれる（なお、チャネル送信契約情報では、契約フラグを設けない構成を採用してもよい）。コンテンツ利用情報は、例えば、図４に示すように有効期限情報、回数制限情報、機器限定情報を含む。

【００４０】チャネル契約情報の改ざんを防ぐ目的で、チャネル契約情報は、暗号化されて放送配信される。また、不利なチャネル契約情報の不取得（例えば契約解除のために放送配信されるチャネル契約情報の不受信もしくは廃棄等）を防ぐ目的で、チャネル契約情報を、他の情報とセットにして暗号化することもできる（この結果、それらはセットで放送される）。

【００４１】本実施形態では、チャネル受信契約情報を含む情報を（その一部または全部が暗号化されているか

否かにかかわらず）「受信契約関連情報」と呼ぶ。なお、チャネル受信契約情報は、それが適用される放送受信機の受信装置ＩＤと一体のものであるので、受信契約関連情報には該受信装置ＩＤも含まれる。また、チャネル送信契約情報を含む情報を（その一部または全部が暗号化されているか否かにかかわらず）「番組関連情報」と呼ぶ。

【００４２】なお、暗号化されて放送されるコンテンツを復号するために必要なチャネルキーは、第１の実施形態では、番組関連情報に含めて（チャネル送信契約情報とともに暗号化されて）放送され、第２の実施形態では、受信契約関連情報に含めて（チャネル受信契約情報とともに暗号化されて）放送される。また、第２の実施形態では、チャネル送信契約情報はコンテンツに付加して（コンテンツとともに暗号化されて）放送される。すなわち、第２の実施形態では、番組関連情報は使用しない。

【００４３】放送受信装置内部で限定受信の仕組みを実現するハードウェアを「限定受信チップ」と呼ぶ。限定受信チップは、限定受信のための秘密情報をその内部に含むことになるので、その内部のメモリやハード構成に関して外部から容易に読み出し、書き込み、変更ができないように、一体化したＬＳＩとして構成し、耐タンパ構造を有することを仮定している。限定受信チップ内部のメモリには、マスター鍵および機器マスター鍵が含まれているものとする。マスター鍵は、主にチャネル受信契約情報を復号するために用いられる。マスター鍵は、第１の実施形態では、放送受信装置に固有とし、第２の実施形態では、全放送受信装置に共通としている。機器マスター鍵は、放送受信装置と２次利用装置との間で共有される鍵で（各２次利用装置が機種毎に定められた機器マスター鍵を有する形態や、全ての２次利用装置が共通の機器マスター鍵を有する形態などが考えられる）、放送受信装置から２次利用装置に転送するコンテンツを暗号化するために用いられる。また、受信装置ＩＤは、受信装置毎個別に設定され、限定受信チップ内部の不揮発性メモリの中に記録されているものとする。

【００４４】本実施形態の放送受信装置で受信されるチャネルは、「通常チャネル」と「契約情報チャネル」に大別することができる。通常チャネルには通常の放送コンテンツを載せたパケットが多重化されて流されている。契約情報チャネルには、受信契約関連情報を載せたパケットや、番組関連情報を載せたパケットが流れている。なお、契約情報チャネルでは、各情報はそれが変更されたときにだけ放送されるのではなく、同じ内容の情報が、例えば一定期間、繰り返し放送される。本実施形態の放送受信装置は、その動作中において、上記のような契約情報チャネルと１つ以上の通常チャネルを常時受信するものである。

【００４５】（第１の実施形態）本実施形態では、各放送受信装置が個別のマスター鍵を有する方式を想定する。このような方式は、各放送受信装置に対し、定期的にしかも個別に受信契約関連情報等を暗号化して送信するので、限定受信のための情報の送信量は比較的大きいが、マスター鍵が破られた際の被害範囲が狭いなど、安全性が非常に高い（このような方式は、ＣＳ放送その他で採用されてきている）。

【００４６】以下、本実施形態の放送受信装置について説明する。

【００４７】図１に、本実施形態に係る放送受信装置の構成例を示す。

【００４８】図１に示されるように、本放送受信装置は、受信部１０１、Ａ／Ｄ変換部１０２、誤り検出／訂正部１０３、チャネル選択部１０４、チャネル選択インタフェース（Ｉ／Ｆ）１０５、限定受信処理部（限定受信チップ）１０６、コンテンツ利用法選択インタフェース（Ｉ／Ｆ）１０７、コンテンツ利用条件表示部１０８を有する。また、限定受信処理部１００すなわち限定受信チップには、フィルター部１１１、デスクランブル部１１２、番組関連情報復号部１１３、受信契約関連情報認証部１１４、受信契約関連情報復号部１１５、受信契約判定部１１６、利用条件判定／修正部１１７、コンテンツ出力制御部１１８、チャネル情報入力部１１９、標準出力部１２０、２次利用出力部１２１、マスター鍵格納部１２２、受信装置ＩＤ格納部１２３、ワーク鍵格納部１２４、チャネルキー格納部１２５、チャネルキー出力部１２６、受信契約情報格納部１２７、送信契約情報格納部１２８が作り込まれ、耐タンパー性が付与されている。

【００４９】次に、本実施形態の暗号化機構について説明する。

【００５０】本実施形態の放送コンテンツは、図５に示すように、３段の暗号化機構によって保護される。

【００５１】まず、上記のように、各放送受信装置は固有のマスター鍵K_Mを持つ。

【００５２】ワーク鍵$K_{W\,ALL}$、チャネル毎に定められる、全ての放送受信装置に共通の鍵である。あるチャネルに対応するワーク鍵K_Wは、送信対象となる放送受信装置に固有のマスター鍵K_Mでワーク鍵識別子とともに暗号化され、対応するチャネル識別子および対象となる受信装置ＩＤとともに送信される。あるいは、マスター鍵K_Mでワーク鍵識別子および対応するチャネル識別子とともに暗号化され、対象となる受信装置ＩＤとともに送信されるようにしてもよい。この結果、送信すべき暗号化ワーク鍵は、放送受信装置毎かつそのチャネル毎に存在する。各放送受信装置では、自装置のマスター鍵K_Mを用いて暗号化されたワーク鍵K_Wを復号し、ワーク鍵識別子およびチャネル識別子と対応付けて記憶する。

【００５３】チャネルキー$K_{c\,n}$は、スクランブル（暗号化）された放送コンテンツをデスクランブル（復号）

するための鍵であり、チャネル毎に定められる。チャネルキーK_{ch}は、対応するワーク鍵K_wでチャネルキー識別子とともに暗号化され、ワーク鍵識別子、および対応するチャネル識別子とともに放送配信される。各放送受信装置では、対応するワーク鍵K_wを用いて暗号化されたチャネルキーK_{ch}を復号し、チャネルキー識別子およびチャネル識別子と対応付けて記憶する。

【００５４】放送コンテンツは、チャネルキーK_{ch}を使って主に共有鍵暗号方式で暗号化され、チャネルキー識別子およびチャネル識別子とともに放送配信される。

【００５５】各放送受信装置では、対応するチャネルキーK_{ch}を用いて、該放送コンテンツを復号することができる。

【００５６】ここで、チャネルキーは解読を防ぐために例えば１０分程度の短時間で変更するのが望ましい。これを送信するために、個別のマスター鍵を使っていたのでは送信量が膨大となるので、全放送受信装置に共通のワーク鍵を使って送信量を削減している。一方、ワーク鍵も何ヵ月という単位で同じ鍵を使うと危険であるので、例えば１ヶ月という単位で変更するのが望ましく、これを個別のマスター鍵で暗号化して送信する。この仕組みによって、たとえマスター鍵が知られても、ワーク鍵を変更することによって無料視聴を防止することができる。

【００５７】なお、ワーク鍵の配信については、例えば、チャネル受信契約情報に含めて配信する形態、ワーク鍵バケットで配信する形態などが考えられる（本実施形態では、チャネル受信契約情報に含めて配信するものとする）。

【００５８】以下、この限定受信システム上でチャネル受信契約情報とチャネル送信契約情報とを統合することにより詳細な限定受信を実現する例を示す。ここでは、限定受信の詳細な例として、コンテンツ２次利用の限定受信による制御方式を取り上げる。もちろん、２次利用での利用制限を目的とした限定受信は一例であり、コンテンツ毎に異なる利用形態を定めなくてはならないようなシステムにおいては、同様の方式を使用することができる。

【００５９】ところで、コンテンツの２次利用は記録メディアに記録しておくことにより何度でも利用できるような利用形態を含むので、その利用形態はコンテンツの価値などに深く依存する。その意味で、従来の受信契約情報のみによる限定受信であるとチャネル毎にしか管理できないので、例えば、チャネルに様々な価値のコンテンツが流れる場合、それらの価値を反映させた個別の制御ができなかった。この問題は、特に録画装置などの外部装置へ出力する際に顕著であり、従来は、一律にコピープロテクションをかけるか、無制限に２次利用を認めるかのどちらかしかなく、例えばコピープロテクションがかかっているチャネルを相当の対価を払って録画可能

にするような限定受信は存在しなかった。また、今後デジタル放送事業が拡大してデータ放送が事業化され、それに伴って２次利用形態が高度化し、デジタル録画が可能になったり、配信ソフトのＰＣでの実行が可能となってきたような場合には、この問題はより深刻になる。本実施形態では、この問題を、契約者の持つチャネル受信契約情報とコンテンツの持つチャネル送信契約情報を統合することにより実現しようとするものである。

【００６０】まず、チャネル契約情報（チャネル受信契約情報／チャネル送信契約情報）について説明する。

【００６１】本限定受信システムによりコンテンツの２次利用を制御する場合、チャネル受信契約情報（あるいはそれが示す契約状態）には、そのチャネルの契約の有無と、契約ありの場合における、そのチャネルで放送されるコンテンツの利用に対する利用条件（制限内容）と当該チャネルのワーク鍵K_w（ワーク鍵をチャネル受信契約情報に含めて配送する場合）を含む。また、チャネル送信契約情報（あるいはそれが示す契約状態）は、そのコンテンツの利用に対する利用条件を含む。

【００６２】図３に、本実施形態のチャネル契約情報のデータ構造例を示す。（ａ）が、ワーク鍵をチャネル受信契約情報に含めて配送する場合におけるチャネル受信契約情報であり、（ｂ）がチャネル送信契約情報と、ワーク鍵をチャネル受信契約情報に含めて配送しない場合におけるチャネル受信契約情報である。

【００６３】図３（ａ）のチャネル受信契約情報は、チャネル識別子、契約フラグ、ワーク鍵識別子、ワーク鍵、コンテンツ利用形態数、コンテンツ利用形態数だけのコンテンツ利用情報の列からなる。

【００６４】「チャネル識別子」は、当該放送コンテンツがどのチャネルのコンテンツかを示すものである。

【００６５】「契約フラグ」は、チャネル識別子で指定されているチャネルの契約状態を示すビット情報である。

【００６６】「ワーク鍵識別子」は、ここで配信するワーク鍵の識別子である。

【００６７】「ワーク鍵」は、当該チャネルのワーク鍵K_wである。

【００６８】「コンテンツ利用形態数」は、本チャネル契約情報に含まれるコンテンツ利用情報の数を示す。

【００６９】「コンテンツ利用情報」は、コンテンツに対する利用条件に関する情報を示す。

【００７０】なお、契約フラグが１の場合にワーク鍵識別子のフィールドおよびワーク鍵のフィールドを有効としてもよいし（契約フラグが０の場合にも、図３（ａ）のようになる）、契約フラグが１の場合にそれらフィールドをチャネル受信契約情報に含めるようにしてもよい（契約フラグが０の場合には、図３（ｂ）のようになる）。

【００７１】なお、以下では、ワーク鍵に関する説明は

省略する。

【００７２】コンテンツ利用情報は、本実施形態では図４に示すように、「有効期限情報」、「回数制限情報」、「機器制限情報」からなるものとする。「有効期限情報」、「回数制限情報」、「機器制限情報」は、それぞれ、当該コンテンツが利用できる、時間的期限、回数的制限、利用される機器の限定を意味し、全て固定長で予め定められた形式で記述されている。

【００７３】図３（ｂ）のチャネル送信契約情報またはチャネル受信契約情報は、チャネル識別子、契約フラグ、コンテンツ利用形態数、コンテンツ利用形態数だけのコンテンツ利用情報の列からなる。各情報は、上記の通りである。

【００７４】次に、放送される各種データについて説明する。

【００７５】本実施形態の限定受信システムにおいて放送受信装置が受信するデータのうちには、コンテンツパケット、番組関連情報パケット、受信契約関連情報パケットがある。

【００７６】まず、放送コンテンツについて説明する。

【００７７】図６に、コンテンツパケットのデータ構造例を示す。

【００７８】コンテンツパケットは、図６に示すように、情報識別子、チャネル識別子、チャネルキー識別子、放送コンテンツからなっている。

【００７９】「情報識別子」は、当該パケットの種別を示すもので、ここではコンテンツパケットであることを示す識別子を記述する。

【００８０】「チャネル識別子」は、当該放送コンテンツがどのチャネルのコンテンツかを示すものである。

【００８１】「チャネルキー識別子」は、当該放送コンテンツを復号するためのチャネルキーの識別子を示す。

【００８２】「放送コンテンツ」は、生の番組データで、チャネルキー識別子で指定されたチャネルキーK_{ch}で暗号化されている。

【００８３】なお、本実施形態ではこれら全ての情報は固定長で表現されたデータであるとする。

【００８４】次に、番組関連情報について説明する。

【００８５】図７に、番組関連情報パケットのデータ構造例を示す。

【００８６】番組関連情報パケットは、図７に示すように、情報識別子、チャネル識別子、ワーク鍵識別子、チャネルキー識別子、チャネルキー、チャネル送信契約情報からなっている。

【００８７】「情報識別子」は、当該パケットの種別を示すもので、ここでは番組関連情報パケットであることを示す識別子を記述する。

【００８８】「チャネル識別子」は、当該番組関連情報がどのチャネルのものかを示すものである。

【００８９】「ワーク鍵識別子」は、当該番組関連情報パケットがどのワーク鍵K_wによって暗号化されているかを示す情報である。

【００９０】「チャネルキー識別子」は、次に記述されているチャネルキーの識別子である。

【００９１】「チャネルキー」は、チャネル識別子で指定されているチャネルの放送コンテンツの暗号化に使われているチャネルキーK_{ch}を示している。

【００９２】「チャネル送信契約情報（C_s）」は、上記チャネルキーK_{ch}で暗号化されているコンテンツの利用条件を記述したチャネル契約情報である。

【００９３】なお、本実施形態では、これら全ての情報は固定長で表現されたデータであり、チャネルキー識別子、チャネルキー、およびチャネル送信契約情報の範囲がワーク鍵識別子で指定されたワーク鍵で暗号化されている。

【００９４】ここで、本実施形態では、同時刻に放送されているコンテンツと、番組関連情報とが対応するものとする（番組関連情報の放送の開始が、対応するコンテンツの放送の開始に若干先行し、番組関連情報の放送と、対応するコンテンツの放送が同時に終了する場合、番組関連情報の放送の開始および終了が、対応するコンテンツの放送の開始および終了に若干先行する場合、などを含む）。なお、その代わりに、各パケットにコンテンツ識別子を付加して、明示的に対応を取るようにしてもよい。

【００９５】次に、受信契約関連情報について説明する。

【００９６】図８に、受信契約関連情報パケットのデータ構造例を示す。

【００９７】受信契約関連情報パケットは、図８に示すように、情報識別子、受信装置ＩＤ、チャネル受信契約情報、誤り検出コードからなっている。

【００９８】「情報識別子」は、当該パケットの種別を示すもので、ここでは受信契約関連情報パケットであることを示す識別子を記述する。

【００９９】「受信装置ＩＤ」は、当該受信契約関連情報がどの放送受信装置宛てのものかを示すものである。

【０１００】「チャネル受信契約情報（C_R）」は、当該放送受信装置の契約状態を示すチャネル契約情報である。

【０１０１】「誤り検出コード」は、チャネル受信契約情報の誤りを検出するコードである。

【０１０２】なお、本実施形態ではこれら全ての情報は固定長で表現されたデータであり（ただし、前述のように、チャネル受信契約情報が可変になる形態もある）、チャネル受信契約情報から誤り検出コードまでが受信装置ＩＤの示す受信装置のマスター鍵で暗号化されている。

【０１０３】以下、本実施形態の放送受信装置の動作について説明する。

【０１０４】図９～図１２に、本実施形態の放送受信装置の動作手順の一例を示す。

【０１０５】まず、ユーザの操作により手動的にもしくは予約機能等により自動的に、チャネル選択インターフェース１０５で所望のチャネルが選択されるものとする。チャネル選択インターフェース１０５で選択されているチャネル番号は、チャネル選択部１０４へ伝えられ、またチャネル情報入力部１１９から受信契約判定部１１６へ伝えられる。

【０１０６】さて、図９のステップＳ１１において受信部１０１で受信された放送波は、Ａ／Ｄ変換部１０２でＡ／Ｄ変換を施されてデジタルデータにされ（ステップＳ１２）、当該放送受信装置内部で処理可能なパケットに再構築される。そして、誤り検出／訂正部１０３で誤り検出／訂正される（ステップＳ１３）。

【０１０７】誤り検出／訂正された受信パケットはチャネル選択部１０４に送られ、放送コンテンツパケット（図６）については、チャネル選択インターフェース１０５にて選択されたチャネルに対応するもののみが、そして、番組関連情報パケット（図７）および受信契約関連情報パケット（図８）については全パケットが、限定受信処理部１００に送られる。

【０１０８】以降は、パケットの種別に応じて処理が分岐する。

【０１０９】フィルター部１１１では、受信パケットの情報識別子を参照し、コンテンツパケットである場合は（ステップＳ１４）、これをデスクランブル部１１２へ送る（ステップＳ１７，Ｓ１８）。コンテンツパケットを与えられたデスクランブル部１１２では、暗号化コンテンツの復号化のための処理を開始する。

【０１１０】番組関連情報パケットである場合は（ステップＳ１５）、番組関連情報復号部１１３へ送る（ステップＳ１９）。番組関連情報パケットを与えられた番組関連情報復号部１１３では、チャネルキーおよびチャネル送信契約情報の復号化のための処理を開始する。

【０１１１】受信契約関連情報パケットである場合は（ステップＳ１６）、受信契約関連情報認証部１１４へ送る（ステップＳ２０）。すなわち、この受信契約関連情報パケットには受信装置個別のマスター鍵によって暗号化されている部分があるので、復号に先だって自装置宛てのパケットであるか否かを判定する。受信契約関連情報パケットを与えられた受信契約関連情報認証部１１４では、パケット内に含まれる受信装置ＩＤを抽出し、受信装置ＩＤ格納部１２３から取り出した受信装置ＩＤと比較することにより、当該受信契約情報パケットが自装置宛てのものかどうかを判定し、自装置宛ての受信契約情報であれば、受信契約関連情報復号部１１５へ送り、そうでなければ処理を終了する。自装置宛ての受信契約関連情報パケットを与えられた受信契約関連情報復号部１１５では、チャネル契約情報の復号化のための処理を開始する。

【０１１２】次に、コンテンツパケットに関する処理について説明する。

【０１１３】受信コンテンツパケットを受け取ったデスクランブル部１１２では、図１０に例示したような手順で処理を行う。

【０１１４】フィルター部１１１からデスクランブル部１１２へ送られたコンテンツパケットは、チャネルキー出力部１２６に対して、チャネル識別子およびチャネルキー識別子を送り、チャネルキーの出力を要請する（ステップＳ３１）。チャネルキー出力部１２６ではこの要請を受けて、受信契約判定部１１６に対して、チャネル識別子を送り、チャネルキーの出力の可否を問い合わせる（ステップＳ３２）。受信契約判定部１１６ではこの問い合わせに応じて、受信契約情報格納部１２７から当該チャネルの受信契約情報を引き出し（ステップＳ３３）、契約フラグが１であれば許可、０であれば不許可を示す信号をチャネルキー出力部１２６に送る（ステップＳ３４～Ｓ３７）。

【０１１５】チャネルキー出力部１２６では、送られてきた可否の判定結果が許可であれば、チャネルキー格納部１２５から当該チャネルの当該チャネルキー識別子を保持したチャネルキーを得てデスクランブル部１１１へ送信し（ステップＳ３８）、不許可であれば、そこで当該コンテンツパケットに関する処理を終了する。

【０１１６】なお、コンテンツパケットはパケットの中でも最も処理頻度が高いので、パケット毎に同様の処理を繰り返すと処理に時間がかかるため、以下の処理を行うと便利である。すなわち、同一チャネルの同一チャネルキーを用いている限りは一回チャネルキーの出力許可がおりたならば、毎回受信契約判定部１１６に問い合わせずにチャネルキーを出力するようにすると便利である。実際、チャネルキーはセキュリティー上の理由で数分に１回変更されるため、このようにしても限定受信に与える影響は少ない。

【０１１７】チャネルキーK_{ch}の出力を受けたデスクランブル部１１２では、コンテンツパケットの暗号化部分を復号して（ステップＳ３９）、コンテンツ出力制御部１１８へ送る（ステップＳ４０）。

【０１１８】コンテンツ出力制御部１１８では、コンテンツ利用方法選択Ｉ／Ｆ１０６を介して、ユーザから入力された当該チャネルのコンテンツ利用方法（例えば、コンテンツ利用条件や利用形態等の情報を含む）を取得し、その利用方法が可能か否かを判定する（ステップＳ４１）。この判定は、利用条件判定／修正部１１７で行われる。なお、この判定処理については後に詳しく説明する。

【０１１９】利用条件判定／修正部１１７で利用許可された場合、その利用形態が標準出力（標準利用のための標準利用装置に対する出力）か２次利用出力かに従って

それぞれ標準出力部１２０、２次利用出力部１２１に出力される（ステップＳ４２）。

【０１２０】その利用形態が標準出力である場合、標準出力部１２０では、当該コンテンツを標準利用装置に対して出力する（ステップＳ４３）。

【０１２１】一方、その利用形態が２次利用出力である場合、２次利用出力部１２１では、利用形態を反映したライセンス情報を生成し（ステップＳ４４）、ライセンス情報をコンテンツにリンクさせて２次利用装置へ出力する（ステップＳ４５）。なお、詳しくは後述するが、コンテンツは２次利用装置との間で共有する機器マスター鍵K_mで暗号化して出力する。なお、ライセンス情報の生成処理については後に詳しく述べる。

【０１２２】次に、利用条件判定／修正部１１７の動作を図１１（判定処理）、図１２（修正処理）に示すフローチャートに沿って説明する。

【０１２３】図１１は、ユーザの所望するコンテンツ利用条件を修正なしに許可できるか否かを判定する部分の処理手順の一例である。

【０１２４】利用条件判定／修正部１１７は、当該チャネルのコンテンツ利用条件が入力されると、受信契約情報格納部１２７から当該チャネルの受信契約情報を取得する（ステップＳ５１）。

【０１２５】受信契約情報格納部１２７において、チャネル受信契約情報は、例えば図１３に示すような形式で格納されている。

【０１２６】有効期限情報は、当該チャネルで放送されたコンテンツの利用可能な有効期限を示す。図１３における有効期限情報は簡単のため「年．月．日」の形式で記述しているが、実際には一つの整数値で表されるものとする。ここで、有効期限情報が“－１”の場合は、有効期限に制限がないことを示し、有効期限情報が“０”の場合は、有効期限が無指定で、即時的にしか有効でないことを示すものとする。

【０１２７】回数制限は、当該チャネルで放送されたコンテンツを使用して良い回数を示す。また、上記と同様に、“－１”は無制限（何回使用しても良い）を、“０”は無指定で、即時的にしか有効でない（例えば放送時に視聴のみ可能）を示すものとする。

【０１２８】機器限定情報については、０が機器を限定しない、１が機器を限定する、を意味するものとする。また、それぞれのチャンネル受信契約情報に指定されている有効期限情報、回数制限情報、機器限定情報は、そのＡＮＤ条件で１つの契約状態を表している。例えば、図１３の例において上から３番目の契約条件は２０００年１月７日まで１０回までどの機器でも視聴することができることを意味している。

【０１２９】当該チャネルのチャネル受信契約情報を取得したら、その個数を計算し、変数ＣＲＭＡＸに格納する（ステップＳ５２）。

【０１３０】同様に、利用条件判定／修正部１１７は、送信契約情報格納部１２８から当該チャネルの送信契約情報を取得する（ステップＳ５３）。

【０１３１】送信契約情報格納部１２８において、チャネル送信契約情報は、例えば図１４に示すような形式で格納されている。図１４における各情報の意味は上記のチャネル受信契約情報と同様である。

【０１３２】当該チャネルのチャネル送信契約情報を取得したら、その個数を計算し、変数ＣＳＭＡＸに格納する（ステップＳ５３，Ｓ５４）。

【０１３３】次に、チャネル受信契約情報を順次チェックし、入力されたコンテンツ利用条件に合致する条件を探す（ステップＳ５５～Ｓ５９）。

【０１３４】例えば、ユーザの所望するコンテンツ利用条件が「１９９９年６月９日まで回数制限なし、機器限定なし、で視聴したい」であれば、図１３の例では、１番目のチャネル受信契約情報に合致する。

【０１３５】合致するものがあった場合には、同様に、チャネル送信契約情報を順次チェックし、入力されたコンテンツ利用条件に合致する条件を探す（ステップＳ６０～Ｓ６４）。

【０１３６】そして、合致するものがあった場合には、当該コンテンツ利用条件を許可する（ステップＳ６５）。

【０１３７】すなわち、ユーザの所望するコンテンツ利用条件を満たすチャネル受信契約情報およびチャネル送信契約情報が存在すれば、当該コンテンツ利用条件を許可する旨の信号をコンテンツ出力制御部１１８に送信して、判定処理を終了する。

【０１３８】一方、チャネル受信契約情報とチャネル送信契約情報の少なくとも一方に合致するものがなかった場合には、不許可を示す信号をコンテンツ出力制御部１１８に送信して判定処理を終了するようにしてもよいが、本実施形態では、コンテンツ利用条件を修正して許可を出すようにしている。

【０１３９】例えば、上記のコンテンツ利用条件「１９９９年６月９日まで、回数制限なし、機器限定なし、で視聴したい」の場合には、図１４の例では、合致するチャネル送信契約情報がないので、このままでは許可することができない。以下のように、利用条件を修正する処理を行う。

【０１４０】図１２は、コンテンツ利用条件の修正が必要となった場合の処理手順の一例である。

【０１４１】この場合は、まず、チャネル受信契約情報とチャネル送信契約情報とを統合して、利用可能な契約情報のリスト（以下、利用可能契約情報リスト）を作る（ステップＳ７１）。

【０１４２】利用可能契約情報リストは、例えば、図１３のようなチャネル受信契約情報のうちの１つのチャネル受信契約条件および図１４のようなチャネル送信契約

情報のうちの１つのチャネル送信契約条件について３つの個別条件毎のＡＮＤ条件をとって契約条件を作成する処理を、全てのチャネル受信契約条件とチャネル送信契約条件との組み合わせについて行うことにより、作成される。図１５に、図１３に示すチャネル受信契約情報と図１４に示すチャネル送信契約情報を統合して得た利用可能契約情報リストの一例を示す。

【０１４３】以下、利用可能契約情報リストの中から、ユーザが所望するコンテンツ利用条件に最も近い条件を抽出する統合処理について説明する。

【０１４４】ここでは、個別条件に優先順位を付け、その優先順位に従って統合されたコンテンツ利用条件に順位を付加し、最も順位の高い契約利用条件を修正利用条件とする方式を採用する。また、優先順位として、「回数制限」→「有効期限」→「機器限定」の順が設定されているものとする。すなわち、この順番で入力されたコンテンツ利用条件に適合するものを探し、最も有利と評価されるものを検索するわけである。

【０１４５】まず、本例では回数制限が１番目に優先されているので、回数制限から利用可能契約情報リストを参照する（ステップＳ７２）。上記のコンテンツ利用条件「１９９９年６月９日まで、回数制限なし、機器限定なし」の場合には、回数制限が無制限（－１）であるため、図１５に示す利用可能契約情報リストの中から回数制限が指定されていないものがあるかどうかをチェックし、ある場合にはそれらを抽出したリストを作成する（ステップＳ７４）。図１５の例では、回数制限が無制限である利用可能契約情報があるので、それらを取り出し、図１６に示すようなリストを作成する。

【０１４６】なお、条件を満たすような利用可能契約情報が無かった場合には、利用可能契約情報リストの中で最も回数制限情報の指定数の多いものを抽出して、同様にリストを作成する（ステップＳ７３）。

【０１４７】次に、本例では有効期限が２番目に優先されているので、抽出されたリストを参照し（ステップＳ７５）、該リストの中から有効期限がコンテンツ利用条件を満たすものを抽出する（ステップＳ７７）。図１６の例の場合には、２番目の利用可能契約情報「１９９９年６月１０日まで回数制限なし、機器限定あり」が抽出される。もちろん、複数の利用可能契約情報が抽出される場合もある。

【０１４８】一方、有効期限が利用条件を満たすような利用可能契約情報がなければ、抽出されたリストの中から有効期限が最も長い利用可能契約情報を抽出する（ステップＳ７６）。

【０１４９】最後に、最も期間の長い契約条件を抽出し、これと入力されたコンテンツ利用条件とのＡＮＤを取ることにより、修正されたコンテンツ利用条件を作成し、これをコンテンツ出力制御部１１８とコンテンツ利用条件表示部１０７に出力する（ステップＳ７８）。

【０１５０】本例の場合、入力利用条件に最も近い（修正された）利用条件は、ユーザ所望の条件「１９９９年６月９日まで、回数制限なし、機器限定なし」と抽出された統合利用条件「１９９９年６月１０日まで、回数制限なし、機器限定あり」とのＡＮＤから、「１９９９年６月９日まで、回数制限なし、機器限定あり」となる。すなわち、本例では、機器限定なしの条件では不許可となるところを、機器限定の条件を付加する修正を行うことによって、ユーザの希望を最大限に満たした上で、許可が得られるようになっている。

【０１５１】コンテンツ出力制御部１１８に出力されたコンテンツ利用条件は、２次利用出力部１２１に送られ、後述する処理によって、当該コンテンツの利用方法を記述したライセンス情報に反映される。

【０１５２】また、コンテンツ利用条件表示部１０７では、入力された利用条件を表示する。本実施形態においては、希望利用条件が修正される場合があるので、ユーザへの利用条件の提示という意味で重要である。

【０１５３】なお、許可できる修正利用条件が得られないような場合には、例えば、不許可にして処理を終了してもよいし、あるいはユーザに希望するコンテンツ利用条件の変更を促すメッセージを表示するようにしてもよい。

【０１５４】このようにすることで、チャネル受信契約情報とチャネル送信契約情報とを統合し、当該チャネルに対して契約者が持っているチャネル受信契約による利用条件と個々のコンテンツに対する利用条件とを統合することことができ、契約者とコンテンツのペア毎に様々な限定受信を実現することができる。このことにより、従来は十分にできていなかったコンテンツの２次利用などへも限定受信を拡張することができる。

【０１５５】次に、２次利用のためのライセンス情報について説明する。

【０１５６】この処理は、コンテンツ利用条件を、ライセンス情報というコンテンツにリンクしたデータとして、実現するものである。

【０１５７】図１７に、ライセンス情報の構成例を示す。

【０１５８】図１７に例示するように、ライセンス情報は、コンテンツＩＤ、コンテンツ利用条件、コンテンツ鍵Ｋｃからなっている。

【０１５９】「コンテンツＩＤ」は、２次利用出力部１２１内で生成される、コンテンツの識別子であり、コンテンツとライセンス情報とを形式的にリンクする役割を持つ。

【０１６０】「コンテンツ利用条件」は、当該コンテンツＩＤのついたコンテンツを利用できる条件である。本実施形態では、コンテンツ利用条件は、図１８に示すように、「有効期限」、「利用回数」、「機器ＩＤ」からなるものとする。有効期限と利用回数は、チャネル契約

情報と同様に、無制限を－１、無指定を０で表すものとする。また、機器ＩＤは、０で機器限定なしを表し、０以外の値で機器限定あり表し、また、本実施形態では、０以外の機器ＩＤは、２次利用される機器の内部に書き込まれているＩＤを示すものとする。

【０１６１】なお、先の処理で最終的に決定されたコンテンツ利用条件（ユーザが最初に入力した条件もしくは修正された条件）と、ライセンス情報におけるコンテンツ利用条件（図１７、図１８）とを区別するために、ライセンス情報におけるコンテンツ利用条件を２次利用条件と呼ぶものとする。

【０１６２】このライセンス情報における２次利用条件は、コンテンツ出力制御部１１８から入力されたコンテンツ利用条件をもとに生成／決定される。

【０１６３】「コンテンツ鍵K_c」は、コンテンツＩＤで指定されるコンテンツを復号するための鍵である。

【０１６４】ライセンス情報は、２次利用条件からコンテンツ鍵までの範囲が、機器マスター鍵K_mで暗号されている。

【０１６５】次に、２次利用のためのコンテンツ情報について説明する。

【０１６６】図１９に、コンテンツ情報の構成例を示す。

【０１６７】図１９に示されるように、コンテンツ情報は、コンテンツＩＤとコンテンツからなり、コンテンツの部分のみがコンテンツ鍵K_cで暗号化されている。

【０１６８】ここで、コンテンツ鍵K_cは、ライセンス情報に暗号化して含まれており、これが実質的なライセンス情報とコンテンツとのリンクになっている。すなわち、ここでは機器マスター鍵K_mは２次利用装置に厳重に秘匿されており、ユーザには知られることがないと仮定している。このため、コンテンツ鍵は機器マスター鍵がなくては取得できず、コンテンツ鍵を取得できるのは２次利用装置であるため、コンテンツとライセンス情報とは「コンテンツを復号するためにはライセンス情報が必要である」という意味でリンクされている。さらに、コンテンツ鍵は、２次利用条件と一緒に暗号化されているため、２次利用条件も同様にコンテンツにリンクされるばかりか、ライセンス情報を偽造すればコンテンツ鍵も破壊されるため、実質的に２次利用条件の改竄も不可能となる。本実施形態では、このようにライセンス情報という形で、コンテンツ利用条件の２次利用への反映を行う。

【０１６９】さて、２次利用出力部１２１は、コンテンツ出力制御部１１８から与えられたライセンス情報およびコンテンツをもとに、２次利用のためのライセンス情報と暗号化コンテンツを作成する。

【０１７０】図２０に、２次利用出力部１２１の構成例を示す。図２０に示されるように、２次利用出力部１２１は、コンテンツ入力部２０１、コンテンツ暗号化部２０２、コンテンツ出力部２０３、コンテンツキー生成部２０４、利用条件入力部２０５、利用条件生成部２０６、コンテンツＩＤ生成部２０７、ライセンス情報生成部２０８、機器マスター鍵格納部２０９、ライセンス情報出力部２１０を含む。

【０１７１】まず、２次利用のためのライセンス情報作成処理について説明する。

【０１７２】図２１に、２次利用のためのライセンス情報の作成手順の一例を示す。

【０１７３】まず、利用条件入力部２０５からコンテンツ利用条件が入力される（ステップＳ８１）。入力されたコンテンツ利用条件は、直ちに利用条件生成部２０６に送られ、当該コンテンツ利用条件に対応するコンテンツのコンテンツＩＤとコンテンツキーK_cの生成をそれぞれコンテンツＩＤ生成部２０７、コンテンツキー生成部２０４に要請し、それぞれが生成を行う（ステップＳ８２，Ｓ８３）。また、コンテンツ利用条件を参照し（ステップＳ８４）、コンテンツ利用条件に機器限定情報がある場合には、機器ＩＤを２次利用装置から取得する（ステップＳ８５）。

【０１７４】次に、入力されたコンテンツ利用条件（および機器限定情報がある場合における機器ＩＤ）から、２次利用条件を作成する（ステップＳ８６）。

【０１７５】次に、機器マスター鍵K_mを機器マスター鍵格納部２０９から取得し（ステップＳ８７）、作成された２次利用条件とコンテンツキーを機器マスター鍵K_mで暗号化し、コンテンツＩＤを付加することにより、ライセンス情報を作成する（ステップＳ８８）。

【０１７６】なお、機器マスター鍵の管理形態には、例えば、各２次利用装置が機種毎に定められた機器マスター鍵を有する形態（機器マスター鍵格納部２０９には、機種ＩＤ毎に対応した機器マスター鍵が格納される）、全ての２次利用装置が共通の機器マスター鍵を有する形態（共通の機器マスター鍵が格納される）などが考えられ、例えばステップＳ８７においては上記の形態に応じて、対象となる２次利用装置の機種ＩＤに対応する機器マスター鍵、あるいは全ての２次利用装置に共通の機器マスター鍵を取得するようにすればよい。また、例えば、各２次利用装置が個別に定められた機器マスター鍵を有するようにすることもできる。

【０１７７】最後に、作成されたライセンス情報を出力する（ステップＳ８９）。

【０１７８】次に、コンテンツ暗号化処理について説明する。

【０１７９】図２２に、コンテンツ暗号化の処理手順の一例を示す。

【０１８０】コンテンツは、コンテンツ入力部２０１から入力されると（ステップＳ９１）、直ちにコンテンツ暗号化部２０２に送られる。コンテンツ暗号化部２０２は、生成されたコンテンツキーをコンテンツキー生成部

２０４から取得し（ステップＳ９２）、コンテンツを暗号化する（ステップＳ９３）。暗号化されたコンテンツは、コンテンツ出力部２０３から出力される（ステップＳ９４）。

【０１８１】なお、図１９の暗号化されたコンテンツおよび図１７の暗号化されたライセンス情報を受信した２次利用装置では、例えば、自装置の機器マスター鍵K_mでライセンス情報を復号してコンテンツ利用条件（図１８）およびコンテンツキーK_cを取り出し、コンテンツ利用条件に含まれる機器ＩＤが０または自装置の機器ＩＤを示しており且つコンテンツ利用条件に含まれるその他の条件が満たされていることを確認した後に、暗号化されたコンテンツをコンテンツキーK_cで復号し、録画や再生などの所定のコンテンツ利用を行う。２次利用装置では、コンテンツの利用にあたっては、ライセンス情報内のコンテンツ利用条件に従って、利用に対するコントロールを行う。例えば、有効期限や利用回数の管理を行う。また、コンテンツおよびそのライセンス情報を、ある２次利用装置から他の２次利用装置に転送可能としてもよい。

【０１８２】このようにすることにより、機器限定されていない場合、当該コンテンツは、他の２次利用機器でも利用できるようになる。

【０１８３】また、標準出力部１２０から標準利用装置にコンテンツを出力する際に、その利用がコンテンツの蓄積を伴うものである場合には、２次利用装置と同様に扱うようにしてもよい。この場合には、コンテンツ利用条件（図１７）については暗号化しないで渡すようにしてもよい。また、放送受信装置と２次利用装置との間で認証手続きを行うようにする場合においても、放送受信装置と標準利用装置との間では認証を省くようにしてもよい。

【０１８４】このようにすることにより、契約者のチャネル受信契約情報とコンテンツに付随するチャネル送信契約情報とを統合し、契約者とコンテンツの利用条件の組合せで詳細な利用形態を実現することができる。また、特に本実施形態では、利用条件として２次利用での利用条件を考えてコンテンツ利用条件を作成し、そのコンテンツ利用条件をライセンス情報という形でコンテンツとリンクし、２次利用装置での利用を利用条件に制限するようなシステムを実現することができる。

【０１８５】さて、以下では、番組関連情報パケットに関する処理（図９のＢの続き）について説明する。

【０１８６】図９の全体処理の流れを示したフローチャートにおいて、受信パケットが番組関連情報パケットであった場合、フィルター部１１１を通して、番組関連情報復号部１１３に送られる。

【０１８７】図２３に、以降の処理手順の一例を示す。

【０１８８】この場合、まず、対応するワーク鍵を、当該パケットに付加されたチャネル識別子およびワーク鍵識別子をキーにして、ワーク鍵格納部１２４から取得する（ステップＳ１０１）。なお、対応するワーク鍵がワーク鍵格納部１２４内に存在しなかった場合は、処理を終了する。

【０１８９】ワーク鍵が取得できた場合には、取得したワーク鍵を使って、番組関連情報を復号する（ステップＳ１０２）。

【０１９０】復号された番組関連情報の中からチャネル送信契約情報C_sを取得し（ステップＳ１０３）、これをチャネル識別子とともに送信契約情報格納部１２８に格納する（ステップＳ１０４）。ここで、チャネル送信契約情報は、放送コンテンツによって変更されるので、本実施形態では、送信契約情報格納部１２８において、同一のチャネル識別子を持つチャネル送信契約情報は常に上書きされるものとする。もちろん、全く同じ情報を上書きするのを省くために、既に存在するチャンネル送信契約情報と比較し、同一でない場合にのみ上書きするようにしてもよい。

【０１９１】以下では、受信契約関連情報パケットに関する処理（図９のＣの続き）について説明する。

【０１９２】図９の全体処理の流れを示したフローチャートにおいて、受信情報が受信契約関連情報パケットであった場合、フィルター部１１１を通して受信契約関連情報認証部１１４に送られる。

【０１９３】図２４に、以降の処理手順の一例を示す。

【０１９４】この場合、まず、受信装置ＩＤ格納部１２３から受信装置ＩＤを抽出し（ステップＳ１１１）、これと受信契約関連情報パケットに含まれる受信装置ＩＤとを比較することにより、当該チャネル受信契約情報が自装置宛てのものであるか否かを判定する（ステップＳ１１２）。自装置宛てのものでなかった場合には、処理を終了する。

【０１９５】自受信装置のものであった場合には、放送受信装置に個別に設定されているマスター鍵K_Mをマスター鍵格納部１２２から取得し（ステップＳ１１３）、受信契約関連情報パケットの暗号化部分を復号する（ステップＳ１１４）。

【０１９６】復号したチャネル受信契約情報から誤り検出コードを取得し、その誤り検出コードを検証することにより、当該チャネル受信契約情報が正しいものであることを確認することができる。

【０１９７】ここで、誤り検出コードを付加して送信し、放送受信装置側でこれを確認しているのは、受信契約関連情報パケットの中で暗号化されていない受信装置ＩＤを偽造して偽の受信契約関連情報を作成し、入力されることを防ぐためである。誤り検出コードはチャネル受信契約情報から導出されるものであり、チャネル受信契約情報を暗号化したまま改変して、偽造しようとしても復号した際、得られたチャネル受信契約情報から導出された誤り検出コードと復号の結果得られた誤り検出コ

ードが一致することは極めて稀であり、偽造防止を防ぐことができる。実際、誤り検出コードがないと暗号化されたチャネル受信契約情報を適当に改変することにより、復号した結果が以前よりも良い契約情報（契約内容）になっている可能性は高く、このような攻撃が容易に成功してしまう。

【０１９８】誤り検出コードが検証されたら（ステップＳ１１５）、受信契約関連情報パケットからワーク鍵K_wと受信契約情報C_Rを取得し（ステップＳ１１６）、それぞれワーク鍵格納部１２４、受信契約情報格納部１１６に格納する（ステップＳ１１７）。

【０１９９】次に、本実施形態の幾つかのバリエーションについて説明する。

【０２００】＜バリエーション１＞まず、コンテンツ利用情報の種類に関するバリエーションについて説明する。

【０２０１】以上では、図４に例示するような、有効期限、回数制限、機器制限からなるコンテンツ利用情報を想定して説明したが、もちろん、利用制限はこれらの他にも種々のものが考えられる。

【０２０２】その一例としては、機種制限のような利用条件が考えられる。これはコンテンツの利用をある機種に限るための条件で、例えば、当該放送コンテンツを特定機種の機器にのみに利用可能にすることによって、特定機種の売上げを促進し、そのために放送契約料金を割安にするなどの運用が可能になる。また、そのような運用以外にも、機種によっては利用条件の管理にセキュリティホールがあり、利用条件が遵守されないことも考えられる。そのような場合に、利用条件に機種制限を入れておくと、そのような機種への２次利用を制限することができる。また、機種限定を入れた場合のライセンス情報には、許可される機種の機種ＩＤを埋め込む方法が考えられる。

【０２０３】また、同様に、コピー防止やコピー回数制限などを利用条件に盛り込むことも可能である。このようにすることによって、２次利用装置からのコピー回数を制限することができる。

【０２０４】＜バリエーション２＞次に、チャネル契約情報の記述方式に関するバリエーションについて説明する。

【０２０５】図４のように情報をそのまま記述する方式（展開形式）の他にも、図２５のように利用条件を制限することを前提にそれをビット列で表現する方式（ビット形式）が使用可能である。図２５（ａ）に示したチャネル受信契約情報や（ｂ）に示したチャネル送信契約情報は、有効期限、コピー回数、機器限定が利用条件として挙がっており、それぞれ、「無制限、１週間、即時」「無制限コピー可、１回コピー可、コピー不可」、「限定なし、限定あり」の条件に制限されており、これらの組合せで表現できる１８通りの条件を対応するビットが

１であることよって表現している。すなわち、若干１８ビットのデータでチャネル契約情報を表現することができる。このような形式のチャネル契約情報を使い、利用条件を統合する際はビット毎の論理積（ＡＮＤ）を使うことにすれば、簡単に統合利用条件を作成することが可能になる。なお、図２５（ｃ）に示す統合利用条件は、チャネル送信契約情報に一致する。

【０２０６】これにより利用条件の修正の際にも効率的に最も良い利用条件を見つけることができる。例えば、「無期限の期間限定で１回コピー可で機器制限のない利用をしたい」という利用条件を、コピー制限、有効期限、機器制限の優先順位で統合する場合、まず１回コピー可の部分（真ん中６ビット）を参照し、そこが０でなければその中で有効期限を比較する。図２５の例では、１回コピー可の条件は認められており、その中で有効期限が無制限のものを探すが、それは存在しない。そこで、許可されている有効期限の中で期間が最も長い１週間のものを選択する。１回コピー可で１週間の有効期限のものは機器限定ありとなしの２種類存在する。ここでは機器制限のない利用を希望しているので、機器制限なしを採用して、「１週間の期間限定で１回コピー可で機器制限のない」利用を統合されたコンテンツ利用条件として決定することができる。

【０２０７】このようにすれば、図１３～図１５のようなリストが不要になり、小さなメモリ領域しかない放送受信装置でも実現されるし、高速処理が可能となる。また、チャネル契約情報が格段に小さくなるため、送信が容易となる。なお、その分契約状態の種類は図１３～図１５のようなリストを用いる場合に比較して制限されるので、使われるシステムの要請によって両者を使い分けると効果的である。

【０２０８】また、システムによってはチャネル受信契約情報が含まれる受信契約関連情報パケットの送信帯域と、チャネル送信契約情報が含まれる番組関連情報パケットの送信帯域が異なっており、どちらか一方の通信路の送信量が少ない場合もある。このような場合には、送信量が少ない方の情報をビット形式で記述し、送信量が多い方を展開形式で記述する方式も考えられる。この場合、ビット形式の契約情報を一旦展開形式に直してマッチングする必要があるため、一般には異なる条件記述形式を統一形式に表現し直す処理を経る必要があり、条件統合の際にはその統一表現を使って前述と同様の手段で統合する。また、このような方式は、番組関連情報パケットとチャネル受信契約関連情報パケットの放送事業者が異なる場合などにも起こる。

【０２０９】＜バリエーション３＞次に、チャネル受信契約情報とチャネル送信契約情報の統合処理に関するバリエーションについて説明する。

【０２１０】前述した統合処理は、各項目に優先順位を付けて、優先度の高い利用条件を採用するものであった

が、各条件をアイテムとした評価関数を定義することによって、よりユーザの希望に近い利用条件を選択することができる。

【０２１１】以下では、評価関数を用いる方式を、ユーザ希望のコンテンツ利用条件が「１９９９年１２月２５日まで、５回まで、機器制限なし」とされた場合を例にとって説明する。

【０２１２】図２６に、この場合の利用条件判定／修正部１１７における処理手順の一例を示す。なお、図２６に示すアルゴリズムは、図１２に示すアルゴリズムと置き換えるものであり、図１１のアルゴリズムから処理が移される。

【０２１３】まず、入力されたチャネル受信契約情報とチャネル送信契約情報を統合して、図１５に示すような利用可能契約情報リストを作成する（ステップＳ１２１）。

【０２１４】次に、作成された利用可能契約情報リストの各々の利用可能契約情報に対して評価値を計算する（ステップＳ１２２）。

【０２１５】まず、基本項目は「有効期限」「回数制限」「機器制限」の３つであり、それぞれ図２７～図２９に示すような基本評価値を与える（図２９の３番目の評価値を０とする考え方もある）。

【０２１６】また、これらの基本評価値を、それぞれw_d, w_t, w_mという関数で置き換え、評価関数を

$f(x) = 10w_d(x) + 5w_t(x) + 2w_m(x)$

のように定義すると、各利用可能契約条件の評価値が図３０のように算出される。

【０２１７】本例の場合は、図３０の評価値の中で最も高い値（１５０）を持つ「２０００年１月７日までに、１０回まで、機器限定で、視聴可能」（図３０における下から２番目）という、利用可能契約情報が選択される（ステップＳ１２３）。本利用可能契約情報は、機器限定以外は、全て上記希望利用条件を満たしている。

【０２１８】ところで、次に高い評価値（１４０）を持つ利用可能契約情報は、「２０００年１月７日までに３回まで機器限定なしで視聴可能」（図３０における下から１番目）であり、回数制限のみが希望利用条件を満たしていない。これらの条件は評価値の差が１０であり、このことからも評価関数や基本評価値の取り方で出力される修正された利用条件の性質を変えることが理解できる。このことが評価関数を用いる利用条件の修正のメリットである。すなわち、利用者は評価関数を自分の好きなように適切に設定することにより、適切な利用条件の修正が自動的に行えるようになることを意味する。

【０２１９】なお、上記の例では希望利用条件で有限回数が指定されているが、希望利用条件で回数無制限が指定された場合には、図２７に示す基本評価値をそのまま使うことができない。このような場合には、利用回数を十分多い上限値、例えば１００回、として計算する方法が考えられる。もちろん、この上限値が十分大きいかどうかは有効期限などの他の条件によって決まる。このため、有効期限などの他の条件を参照した上で、無制限の回数条件が指定された場合に基本評価値を参照する際の有限回数をフレキシブルに設定すると、より正確な利用条件の修正に貢献する。

【０２２０】また、より正確な利用条件を選択するという意味では、ユーザへの問い合わせ機能を持たせると好ましい。それを担うのはコンテンツ利用方法選択Ｉ／Ｆ１０６である。ここでは、コンテンツの希望利用条件を入力する他に、希望利用条件が満たされなかった際、評価値の高い順に利用条件を並び変え、図３１のように表示することによりユーザにコンテンツ利用条件の自主的な選択を促す。

【０２２１】図３２に、上記のような場合の処理手順の一例を示す。

【０２２２】まず、利用条件判定／修正部１１７は、チャネル受信契約情報とチャネル送信契約情報が入力されると、前述のような手段でそれらを統合し、利用可能契約情報リストを作成する（ステップＳ１３１）。

【０２２３】続いて、利用可能契約情報リストにある各々の利用可能契約情報に対して、前述した評価関数を用いて、評価値を算出する（ステップＳ１３２）。

【０２２４】ここで、算出した評価値が高い順に利用可能契約情報を並べ変え（ステップＳ１３３）、並び変えられたリストをコンテンツ出力制御部１１８を経由してコンテンツ利用方法選択Ｉ／Ｆ１０６に送信する（ステップＳ１３４）。

【０２２５】コンテンツ利用方法選択Ｉ／Ｆ１０６では、画面に図３１に例示示するような利用方法選択画面を出力して、ユーザからの利用方法の選択を促す。ここで、評価値の高い順に表示されるので、ユーザは、次画面を表示しなくても、所望に近い利用形態を選択することができ、便利である。

【０２２６】なお、明らかに省略できる条件を特定してそれを省くことにより、より多くの選択子を出力することも可能である。図３１の例の場合、第３・第４の利用条件がそれにあたり、すなわち、第４の条件が第３の条件の有効期限の制限になっており、選択条件としては無駄なものである（すなわち、第４の条件を省く）。これらは、条件を比較することにより決定可能であり、候補数が少なければ特定することは容易である。

【０２２７】＜バリエーション４＞次に、２次利用出力部１２１においてライセンス情報を作成する処理および構成のバリエーションについて説明する。

【０２２８】前述した実施形態では、ライセンス情報を、図１７に例示するようにコンテンツに切り離されたデジタルデータとして扱っていた。しかし、これは出力の際にアナログ変換した後での利用制御には（ライセン

ス情報が切り離されてしまうので）利用できない。すなわち、前述の実施形態では、デジタル録画の制御はできるが、アナログ録画の制御は不可能である。そこで、アナログデータに変換されてもなお、２次利用制御ができる方式が重要となる。

【０２２９】一方で、主に画像や音声などのアナログデータにデータを埋め込む電子透かしという技術が近年注目を集めている（「電子透かしの基礎」（松井甲子雄著、森北出版、１９９８）等参照）。この技術を使うと、情報をアナログデータの中に目立たなく且つ容易には抜き取られないように、埋め込むことができる。すなわち、電子透かし技術を使うと、ライセンス情報をアナログデータの中に埋め込むことができるので、アナログデータになってもなお、利用管理ができるばかりか、物理的に分離されたライセンス情報を持たなくても良いので、管理も簡単である。

【０２３０】以下、電子透かしを使ったライセンス管理について説明する。

【０２３１】図３３に、この場合の２次利用出力部１２１の構成例を示す。図３３に示されるように、２次利用出力部１２１は、コンテンツ入力部２２１、電子透かし埋め込み部２２２、コンテンツ暗号化部２２３、コンテンツ出力部２２４、機器マスター鍵格納部２２５、利用条件入力部２２６、利用条件生成部２２７を含む。

【０２３２】図３４に、この場合の処理手順の一例を示す。

【０２３３】まず、利用条件入力部２２６からコンテンツ利用条件が入力されと（ステップＳ１４１）、利用条件生成部２２７に送られる。利用条件生成部２２７は、入力されたコンテンツ利用条件に機器限定があるかを判定する（ステップＳ１４２）。ここで、機器限定の利用制限がある場合は、図２０および図２１の場合と同様にして、機器ＩＤを２次利用装置から取得し（ステップＳ１４３）、図１８に例示したような形式で、ライセンス情報を生成する（ステップＳ１４４）。機器限定の利用制限がない場合は、そのままライセンス情報を生成する（ステップＳ１４４）。

【０２３４】次に、生成したライセンス情報を電子透かし生成部２２２に送り、コンテンツ入力部２２１から入力されたコンテンツに埋め込む（ステップＳ１４５）。埋め込まれたコンテンツは、コンテンツ暗号化部２２３において、機器マスター鍵格納部２０９から取得した機器マスター鍵K_mで暗号化され（ステップＳ１４６，Ｓ１４７）、コンテンツ出力部２２４から出力される（ステップＳ１４８）。

【０２３５】以上のように構成することにより、処理も構成も簡単になる。なお、電子透かしでは画像の１枚毎に埋め込むので時間を要し、また、新たにライセンスを購入するなどしてコンテンツを再生利用する際には埋め込んだ電子透かしを一旦外して、新たに作成した透かしを埋め込む必要がある（これはライセンス情報がコンテンツ情報と分離していないために起こる）。このような状況においては、お互いの良い点を活かすため、ライセンスに含まれる限定項目の種類によってデジタルライセンスとして反映させるか、電子透かしでアナログレイヤに埋め込むかを決定して、運用するシステム構成も考えられる。

【０２３６】＜バリエーション５＞次に、２次利用装置側の機器信頼性に関して説明する。

【０２３７】本実施形態において、コンテンツ利用条件をライセンス情報という形で出力しても、２次利用装置においてそれが忠実に守られなくては意味がない。これは通常の機器接続においても言えることである。

【０２３８】近年検討されているデジタル機器間の接続に関する国際規格ＩＥＥＥ１３９４では、この点に鑑みて認証プロトコルを導入している。ＩＥＥＥ１３９４規格はデジタル機器間の入出力に関してプロテクション機構を設け、それらが転送されるバス上、接続ケーブル上においてもコピープロテクションすることを規格化している。

【０２３９】そこで、本実施形態において、放送受信装置と２次利用機器との間をＩＥＥＥ１３９４バスで接続し、上記認証プロトコルを利用する方法も考えられる。

【０２４０】以下、バス、接続ケーブルのように機器間のデータ転送に利用される接続線を特に「接続回線」ということにする。

【０２４１】従来のＤＶＤなどに記録される暗号化データは、ＤＶＤ上から生データが直接読み込めないという意味では、コピープロテクションがなされているが、再生する際は、機器内で復号され、（デジタルＴＶなどの）外部機器に生のデータとして出力される。この場合、接続回線上で、当該生データを捕らえれば簡単にコピープロテクションが破られてしまう。このため接続回線上でもコンテンツを保護する立場から、接続機器間で互いに取り決めた暗号鍵によってコンテンツを暗号化して転送することにより、接続回線上でのコピープロテクションを実現しているのが、ＩＥＥＥ１３９４のコピープロテクション規格である。

【０２４２】しかし、いかに通信路上でコピープロテクションを行っても、出力する機器の設計の不備などの理由で暗号化したコンテンツが解読され、コンテンツが生の状態で保存できる状態にあれば意味がない。したがって、相手の機器の機種が別途得られた無効機器リスト（リボケーションリスト）に含まれているか否かを判断し、含まれている場合には、出力を拒絶する。含まれていない場合には、接続されている機器が本当にその機種であるかを確かめるために、チャレンジデータを相手の機器に出力し、当該機種しか知り得ない情報を使って、当該チャレンジデータにデジタル署名を付けてもらい、それを送り返してもらい、その署名を検証することによ

り、認証を行う。

【０２４３】ただし、ここで１つの機器が全ての機種の公開鍵を保持しておくことは現実的ではないので、実際上は接続機器から公開鍵を取得する。ただし、公開鍵は署名の検証鍵でもある一方で、公開鍵と秘密鍵のペアは比較的簡単に生成できる事実があるので、別の機種のマシンが当該機種を偽って公開鍵を送信するというプロテクト破りの手法が考えられる。このため、それぞれの機種は、発売時に、公開鍵と秘密鍵のペアを作成し、ＩＥＥＥ１３９４が定める管理機関に公開鍵を示して、デジタル証明書を発行してもらい、それを送信するという認証方法を採用している。デジタル証明書には管理機関の持つ秘密鍵でデジタル署名が施されており、対応する公開鍵が全ての機器に予め含まれているので、当該公開鍵が含まれるデジタル証明書を認証することにより、当該公開鍵が正しいものかどうかを判断することができる。

【０２４４】また、デジタル署名の作成には、大きく分けて、公開鍵暗号を使う方式と、共通鍵暗号を使う方式があり、前者は後者よりも処理時間がかかるが、安全がより高いため、計算能力の高い（主に据え置き型の）機種、後者は安全性は劣るが、処理能力が低い機種でも実行できるので、計算能力の低い（主に携帯型の）機種に適用される。認証の後は互いに共通に知る情報（例えば公開鍵）を基に鍵の交換プロトコルを実行し鍵を交換し、その鍵を使ってコンテンツを暗号化して転送する。

【０２４５】ＩＥＥＥ１３９４を利用する場合、本実施形態における機器間の転送もＩＥＥＥ１３９４に準拠しなくてはならない。この意味で共通化でき、本実施形態でも必要となるのは機器認証の部分である。すなわち、前述したように、本実施形態において２次利用の制限を行っても、２次利用装置がそれを実行しない、もしくは簡単な改造によって実行されないようにできてしまう場合には、当該機種の機器には２次利用させるべきではない。ただし、この場合であっても、コピープロテクションは正常に動作する可能性もあるので、無効機器リストをＩＥＥＥ１３９４とは別に配布することが望ましい。そのためには、専用にパケットを定義し、放送によって送信すれば効果的である。また、上記でコンテンツの暗号化鍵として定めたコンテンツ鍵Ｋｃをｉｅｅｅ１３９４プロトコルで生成される共有鍵とすることもできる。その場合は、本実施形態の２次利用出力部１２１が作成するコンテンツ鍵Ｋｃで暗号化した上にＩＥＥＥ１３９４が定める転送鍵でさらに暗号化する必要がなくなり、処理を省くことができる。

【０２４６】以下では、上記の認証プロセスを導入した場合のコンテンツ出力制御部１１８について説明する。

【０２４７】図３５に、この場合のコンテンツ出力制御部１１８の構成例を示す。図３５に示されるように、コンテンツ出力制御部１１８は、利用条件入力部３０１、出力判定部３０２、機器認証部３０３、利用情報出力部３０４を含む。

【０２４８】図３６に、この場合の処理手順の一例を示す。

【０２４９】コンテンツ出力制御部１１８の利用条件入力部３９１からコンテンツ利用条件が入力され（ステップＳ１５１）、出力判定部３０２においてコンテンツの出力判定が行なわれる。実際の出力判定は、利用条件判定／修正部１１７により行なわれる。

【０２５０】ここで、利用可能でなく（ステップＳ１５２）、かつ修正不可能ならば（ステップＳ１５３）、利用不許可の出力を２次利用出力部１２１に行ない（ステップＳ１５４）、処理を終了する。

【０２５１】それ以外の場合は、希望通りかもしくは修正された利用条件が得られ（ステップＳ１５２，Ｓ１５３，Ｓ１５５）、出力判定部３０２において、後述する機器認証部３０３の機器認証の結果に基づいてコンテンツを出力して良いか否かの判定を行ない（ステップＳ１５６）、出力可となれば、コンテンツ利用条件を利用条件出力部３０４から２次利用出力部１２１へ出力する（ステップＳ１５７）。出力不許可の場合は、利用不許可の旨を示す信号を２次利用出力部１２１へ出力する（ステップＳ１５４）。

【０２５２】一方、機器認証部３０３は、コンテンツ利用条件が入力された時点から上記のプロセスとは独立に、放送受信装置から２次利用装置の認証を行なう（ステップＳ１５８）。

【０２５３】認証は、まず、２次利用装置から機種ＩＤを出力してもらい、当該機種ＩＤの２次利用装置が安全な装置か否かの判定を受信装置内部に持つ安全でないＩＤの一覧を示したリボケーションリストを参照して行なわれる。ここで、安全な機種であるとされた場合は、接続されている機種が確かに当該ＩＤを持つ機種であるかを確認する。この確認には、デジタル署名技術が用いられる。

【０２５４】デジタル署名技術については、例えば次のような実現形態が考えられる。まず、放送受信装置はランダムに選んだメッセージを２次利用装置に送り、当該ＩＤを持った２次利用装置しか知り得ない秘密情報を使って暗号化して返送してもらう。そして、返送された暗号文を放送受信装置が持つ対応した鍵を使って復号して検証することによって、確かに当該ＩＤを持つ２次利用装置が接続されていることを認証することができる。

【０２５５】ここで、認証されなければ（ステップＳ１５９）、２次利用装置が不認証であった旨の信号を２次利用出力部に出力して終了する（ステップＳ１６１）。認証された場合は、同様の処理を２次利用装置側から行ない（ステップＳ１６０）、放送受信装置は２次利用装置側から送られて来たランダムメッセージを受信装置が持つ認証用の秘密鍵で暗号化して送信する。このことにより、２次利用装置側から受信装置が認証されれば（ス

テップＳ１６３）、利用条件の出力を許可しても良い旨の信号を出力判定部３０２に送る。そうでない場合は、放送受信装置が不認証であった旨の信号を２次利用出力部１２１に送り（ステップＳ１６２）、処理を終了する。

【０２５６】さらに、認証の際、受信装置から２次利用装置を認証するだけの構成も考えられる。一般には、認証は処理時間のかかる処理であるので、片方向だけであると処理が半分となる。また、放送受信装置は放送局から送信されてきたデータを秘密データを使って復号できるという意味からは、既に放送局によって認証されているものと考えることができるからである。

【０２５７】＜バリエーション６＞これまでの説明では、チャネル送信契約情報は、対応するコンテンツと同時性を持って放送されるものとしたが、チャネル送信契約情報を例えばＥＰＧ（Ｅｌｅｃｔｒｏｎｉｃ　Ｐｒｏｇｒａｍ　Ｇｕｉｄｅ：電子番組ガイド）に含めて予め放送するようにしてもよい。

【０２５８】以下では、予めチャネル送信契約情報を放送し、コンテンツの放送に先だって、コンテンツ利用条件を決定可能とした実施形態について、録画予約の際にコンテンツ利用条件を決定する場合を例にとって説明する。

【０２５９】図３７に、録画予約機能を持つ放送受信装置の構成例を示す。本放送受信装置は、基本的には、図１の構成と同様であるので、相違する点についてのみ説明する。

【０２６０】図３８に、チャネル送信契約情報を含む電子番組ガイド情報の構造例を示す。

【０２６１】電子番組ガイド情報パケットは、図７に示すように、情報識別子、チャネル識別子、コンテンツ識別子、チャネル送信契約情報、番組情報からなっている。情報識別子、チャネル識別子、コンテンツ識別子、チャネル送信契約情報は、これまでと同様である。番組情報は、対応するコンテンツに関する情報で、例えば、タイトル、放送開始日時、放送終了日時、ジャンル、出演者といったような情報である。電子番組ガイド情報は、例えば、契約チャネルで放送される。また、電子番組ガイド情報パケットは、暗号化しないものとする。

【０２６２】なお、チャネル送信契約情報は、番組関連情報パケットにも含めてもよいし、電子番組ガイド情報パケットでのみ放送するようにしてもよい。

【０２６３】また、ここでは、コンテンツパケットと、その他のチャネル送信契約情報を含むパケット（コンテンツ対応の情報を含むパケット）には、コンテンツ識別子を付加するものとする。

【０２６４】さて、図３７においては、電子番組ガイド情報パケットを受信した場合、フィルター部１１１から番組関連情報復号部１１３を経由して、番組情報および各識別子がコンテンツ利用法選択Ｉ／Ｆ１０６へ渡され、コンテンツ利用法選択Ｉ／Ｆ１０６において蓄積される。また、チャネル送信契約情報および各識別子が送信契約情報格納部１２８に蓄積される。

【０２６５】そして、例えば、ユーザが録画予約を行う場合、番組指定や録画先などの通常の操作の他に、希望するコンテンツ利用条件の入力を行う。以降は、既に説明した処理と同様にコンテンツ利用条件の判定や修正などが行われ、最終的に当該コンテンツに対するコンテンツ利用条件が決定される。

【０２６６】なお、この時点あるいはそれ以降の適当なタイミングで、ライセンス情報を作成する。

【０２６７】次に、コンテンツ利用法選択Ｉ／Ｆ１０６、録画予約されたコンテンツの放送開始時刻を監視し、あるいは該コンテンツの識別子が受信されたかどうかを監視し、放送開始時刻（もしくはその一定時間前）になった場合、あるいは該コンテンツの識別子が受信された場合に、録画を開始する。すなわち、コンテンツを暗号化し、暗号化コンテンツとライセンス情報を、録画機器に送信する。

【０２６８】以降は、録画機器において、与えられたライセンス情報に従って、コンテンツの利用が行われる。

【０２６９】＜バリエーション７＞次に、チャネル受信契約情報の圧縮手法に関して説明する。

【０２７０】これまでは、チャネルとチャネル受信契約情報が１対１に対応する場合を想定して説明したが、この場合には、サイズ的に比較的大きくなる可能性のあるチャネル受信契約情報を１チャネル毎に対応して配送することから、契約者数、チャネル数、チャネル受信契約情報の大きさ、配信頻度などと、通信路の送信帯域との関係によっては、チャネル受信契約情報の送信量が通信路の送信帯域を圧迫することもある。

【０２７１】そこで、以下では、複数のチャネルに共通のチャネル契約情報を送信する方法について説明する。

【０２７２】ところで、例えばチャネル数の多いＣＳ放送では、数種類のパッケージ（複数のチャネルのセット）を設け、そのパッケージを単位として契約することがほとんどである。

【０２７３】ここでは、このようなシステムに適応することを想定し、図３のチャネル識別子の代わりに、パッケージ識別子を導入する場合を例にとって説明する。

【０２７４】パッケージとは、複数のチャネルのセットのことであり、パッケージ識別子はパッケージを識別するための識別子である。

【０２７５】さらに、当該パッケージ識別子のパッケージにどのチャネルが含まれるかを記述したパッケージ定義情報は別途送信されるものとする。ただし、ここでは説明を簡明にするために、図２に示すようなビット列をパッケージ識別子とする。この場合、ビット列で１が立っているビット位置に対応したチャネル（図２では、２チャネル、５チャネル、７チャネル、８チャネル）が当

該パッケージに含まれているチャネルを意味するものとする。

【０２７６】このようにすることで、複数のチャネルのチャネル受信契約情報をまとめて送信することができるため、送信量削減の観点から有効である。もちろん、このようなシステムにおいても、チャネル毎に個別のチャネル受信契約情報を送信することは可能で、なぜなら、８ビットのうち当該チャネルに対応したビットだけを１にすればよい。

【０２７７】パッケージ識別子を導入するため変更する処理は、図１における受信契約関連情報復号部において、チャネル識別子とチャネル受信契約情報をセットにして受信契約情報格納部に格納していた部分を、パッケージ識別子を解釈して、チャネル毎の記述形式に直し、受信契約情報格納部に格納するように変更すればよい。

【０２７８】また、パッケージ識別子を導入した場合、ワーク鍵との対応が問題になる。この場合、同じパッケージに含まれるチャネルは同じワーク鍵とする方法と、前記のようにワーク鍵がチャネル毎に異なることを前提とし、契約に応じて個別契約者に対応するチャネルのワーク鍵を契約者の放送受信装置が持つマスター鍵で暗号化して別途送信する方式が考えられる。

【０２７９】（第２の実施形態）本実施形態の放送受信装置の２次利用に関する処理および各情報に対する処理等は、基本的には第１の実施形態と同様であるので、以下では相違する点もしくは追加する点を中心に説明する。

【０２８０】第１の実施形態では、各放送受信装置が個別のマスター鍵を有する方式を想定したが、本実施形態では、全ての受信装置が共通のマスター鍵を有する方式を想定して説明する。このような限定受信システムにおいては、各受信装置対し、個別に契約情報を暗号化して送信する必要がないので、限定受信の送信量が少なくてすむという利点がある。また、本実施形態では、デジタル署名などの偽造防止技術を用いて、そのマスター鍵が破られた際の安全性への対策を行っている。

【０２８１】第１の実施形態では、図５のような３段の鍵構成を採用したが、本実施形態では、このような限定受信のために、図３９のような２段の鍵構成を採用する。すなわち、チャネルキーK_{ch}とチャネル受信契約情報を全ての受信装置に共通のマスター鍵K_Mで暗号化して送信する。送信されたチャネルキーを使って放送コンテンツを復号する。

【０２８２】以下、この限定受信システム上で第１の実施形態と同様にチャネル受信契約情報とチャネル送信契約情報とを統合することに限定受信として２次利用に対する制御を実現する例を示す。

【０２８３】第１の実施形態では、放送受信装置は、コンテンツパケット（図６）、番組関連情報パケット（図７）、受信契約関連情報パケット（図８）を受信したが、本実施形態においては、これらに対応するものとして、放送受信装置は、図４０に示すようなコンテンツパケットと図４１に示すような受信契約関連情報パケットを受信する。

【０２８４】コンテンツパケットは、図４０に示されるように、情報識別子、チャネル識別子、チャネルキー識別子、チャネル送信契約情報C_i、放送コンテンツからなっており、チャネル送信契約情報から放送コンテンツまでの部分をチャネルキーK_{ch}で暗号化している。なお、各情報の意味と役割は第１の実施形態と同じであるので、ここではその説明は省略する。

【０２８５】第１の実施形態と相違し、本実施形態においては、チャネル送信契約情報がコンテンツパケットに含まれる。これは鍵構造が２段であることによる必然性もあるが、コンテンツと当該コンテンツのチャネル送信契約情報とが物理的にリンクしているので、システムとしても構成しやすいという利点もある。

【０２８６】受信契約関連情報パケットは、図４１に示されているように、情報識別子、マスター鍵識別子、チャネル識別子、チャネルキー識別子、チャネルキー、契約情報の数ｎ、ｎ個の契約情報、デジタル署名からなっており、チャネル識別子からデジタル署名までの部分をマスター鍵で暗号化している。

【０２８７】デジタル署名は、契約情報数ｎおよび契約情報１～契約情報ｎまでの部分に関してのデジタル署名である。デジタル署名は、契約情報の偽造を防ぐためのものであり、契約情報を１ビットでも変更するとデジタル署名が検証できなくなるという性質を持っている。さらに、デジタル署名を作成するには放送局側にしか存在しない秘密鍵を知らなくてはできないため、デジタル署名を付加することにより契約情報の偽造を防ぐことができる。

【０２８８】ここで、「契約情報」とは、図４２に示されるように、受信装置ＩＤとチャネル受信契約情報からなっており、受信装置ＩＤに対応するチャネル受信契約情報を表している。

【０２８９】なお、受信契約関連情報に含まれるその他の各情報の意味と役割は第１の実施形態と同じであるので、ここではその説明は省略する。

【０２９０】図４３に、本実施形態に係る放送受信装置の構成例を示す。

【０２９１】図４３に示されるように、本放送受信装置は、受信部１０１、Ａ／Ｄ変換部１０２、誤り検出／訂正部１０３、チャネル選択部１０４、チャネル選択インタフェース（Ｉ／Ｆ）１０５、限定受信処理部（限定受信チップ）１０６、コンテンツ利用法選択インタフェース（Ｉ／Ｆ）１０７、コンテンツ利用条件表示部１０８を有する。また、限定受信処理部１００すなわち限定受信チップには、フィルター部１１１、デスクランブル部１１２、受信契約関連情報認証部１１４、受信契約関連

情報復号部１１５、受信契約判定部１１６、利用条件判定／修正部１１７、コンテンツ出力制御部１１８、チャネル情報入力部１１９、標準出力部１２０、２次利用出力部１２１、マスター鍵格納部１２２、受信装置ＩＤ格納部１２３、チャネルキー格納部１２５、チャネルキー出力部１２６、受信契約情報格納部１２７、送信契約情報格納部１２８、送信契約情報抽出部１２９が作り込まれ、耐タンパー性が付与されている。

【０２９２】以下、本実施形態の放送受信装置の動作について説明する。

【０２９３】図４４～図４６に、本実施形態の放送受信装置の動作手順の一例を示す。

【０２９４】本実施形態の放送受信装置は、放送波を受信後（ステップＳ２０１）、Ａ／Ｄ変換を行なってデジタルデータに変換して（ステップＳ２０２）、誤り検出および誤り訂正を行なって（ステップＳ２０３）、フィルター部１１１においてパケット内の情報識別子によってコンテンツパケットであれば（ステップＳ２０４）、チャネル識別子を参照して、視聴チャネルのコンテンツかどうかを判定し（ステップＳ２０５）、視聴チャネルであった場合はデスクランブル部１１２へ送信する（ステップＳ２０６）。そうでない場合は、当該パケットに関する処理を終了する。受信契約関連情報パケットであった場合は（ステップＳ２０７）、契約関連情報に送信する（ステップＳ２０８）。

【０２９５】次に、視聴チャネルのコンテンツパケットの処理に関して図４５のフローチャートに従って詳しく説明する。

【０２９６】コンテンツパケットがデスクランブル部１１２に入力されると、デスクランブル部１１２ではチャネルキー出力部１２６へチャネルキーの出力の要請を行なう（ステップＳ２１１）。チャネルキー出力部１２６では、受信契約判定部１１６に対してチャネル識別子を入力し、受信契約情報格納部１２７から当該チャネルのチャネル受信契約情報を取得して、契約フラグが１である場合、チャネルキーの出力許可信号を出し、０である場合はチャネルキーの出力不許可信号を出す（ステップＳ２１２～２１７）。チャネルキー出力不許可信号が入力された場合、チャネルキー出力部１２６では当該パケットに関する処理を終了する。

【０２９７】チャネルキーの出力許可信号がチャネルキー出力部１２６へ入力された場合は、チャネルキー出力部１２６はチャネルキー格納部１２５へチャネル識別子とチャネルキー識別子を送り、チャネルキーを取得しデスクランブル部１１２へ送り（ステップＳ２１８）、デスクランブル部１１２においてコンテンツのデスクランブルを行なう（ステップＳ２１９）。

【０２９８】送信契約情報抽出部１２９は、デスクランブルされたコンテンツにチャネル送信契約情報が含まれているか否かを情報識別子で判定し（ステップＳ２２０）、含まれている場合チャネル送信契約情報を取得し、送信契約情報格納部１２８へ格納する（ステップＳ２２１）。

【０２９９】次に、コンテンツはコンテンツ出力制御部１１８へ送られ、第１の実施形態と同様の方法で、当該コンテンツについてコンテンツ利用情報をチェックする（ステップＳ２２２）。チェックした結果、利用不許可であれば、コンテンツ利用条件表示部１０７に利用不許可の表示を行ない、処理を終了する。許可された場合は、利用形態とコンテンツとともに標準出力であるか２次利用出力であるかによって（ステップＳ２２３）、それぞれ、標準出力部１２０、２次利用出力部１２１に出力される。

【０３００】２次利用出力部１２１に出力された場合は、第１の実施形態と同様の処理でライセンス情報とそれに対応したコンテンツを生成し（ステップＳ２２４）、２次利用装置に出力して（ステップＳ２２５）、処理を終了する。

【０３０１】次に、受信契約関連情報パケットの処理に関して図４６のフローチャートに従って詳しく説明する。

【０３０２】受信契約関連情報が受信契約関連情報復号部１１４に入力されると受信契約関連情報復号部１１４ではマスター鍵識別子をキーにして、マスター鍵格納部１２２からマスター鍵K_Mを取得して（ステップＳ２３１）、暗号化部分を復号する（ステップＳ２３２）。復号された受信契約関連情報からチャネルキー、チャネル識別子、チャネルキー識別子を抽出し（ステップＳ２３３）、チャネルキー格納部１２５に格納する（ステップＳ２３４）。

【０３０３】次に、契約情報数ｎからデジタル署名までの部分を受信契約情報認証部１１５へ送付する。

【０３０４】受信契約情報認証部１１５では契約情報数ｎを抽出し、それを変数ＭＡＸに代入する。引続き契約情報を次々参照し、それらに含まれる受信装置ＩＤと受信装置ＩＤ格納部１２３にある受信装置ＩＤを比較して（ステップＳ２３６～Ｓ２３９）、一致した場合、デジタル署名を検証後（ステップＳ２４０，Ｓ２４１）、対応するチャネル受信契約情報C_Rを受信契約情報格納部１２７へ格納する（ステップＳ２４２）。自受信装置の受信装置ＩＤと一致する契約情報がない場合や、デジタル署名が検証できなかった場合は、その時点で処理を終える。

【０３０５】なお、第１の実施形態において示したバリエーションは、本実施形態にも適用可能である。

【０３０６】なお、本実施形態において、チップ化しなくてよい処理機能の部分（例えば、ユーザインタフェースに関する部分など）は、ソフトウェアを利用しても実現可能である。また、そのような処理機能の部分は、コンピュータに所定の手段を実行させるための（あるいは

コンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【０３０７】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０３０８】

【発明の効果】本発明によれば、あるチャネルに対して契約者が持っている１または複数の第１の利用条件と、あるコンテンツに対して規定されている１または複数の第２の利用条件とを統合することによって、契約者とコンテンツのペア毎に様々な限定受信を実現することができる。このことにより、コンテンツの価値などに応じてコンテンツ毎に利用制御することが可能になり、また、従来は十分にできていなかったコンテンツの２次利用などへも限定受信を拡張することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る放送受信装置の構成例を示す図

【図２】チャネル展開情報の一例を示す図

【図３】チャネル契約情報のデータ構造例を示す図

【図４】コンテンツ利用情報のデータ構造例を示す図

【図５】放送コンテンツの暗号化機構について説明するための図

【図６】放送コンテンツパケットのデータ構造例を示す図

【図７】番組関連情報パケットのデータ構造例を示す図

【図８】受信契約関連情報パケットのデータ構造例を示す図

【図９】同実施形態に係る放送受信装置における放送受信からパケットの内容に応じた処理までの全体的な処理手順の一例を示すフローチャート

【図１０】放送コンテンツパケットに対する処理手順の一例を示すフローチャート

【図１１】利用条件判定／修正部における処理手順の一例を示すフローチャート

【図１２】利用条件判定／修正部における処理手順の一例を示すフローチャート

【図１３】チャネル受信契約情報におけるコンテンツ利用条件一例を示す図

【図１４】チャネル送信契約情報におけるコンテンツ利用条件の一例を示す図

【図１５】利用可能契約情報リストの一例を示す図

【図１６】抽出結果リストの一例を示す図

【図１７】ライセンス情報のデータ構造例を示す図

【図１８】コンテンツ利用条件の一例を示す図

【図１９】放送受信装置から２次利用装置へ渡される暗号化コンテンツのデータ構造例を示す図

【図２０】２次利用出力部の内部構成の一例を示す図

【図２１】ライセンス情報を作成する処理手順の一例を示すフローチャート

【図２２】コンテンツを暗号化する処理手順の一例を示すフローチャート

【図２３】番組関連情報パケットに対する処理手順の一例を示すフローチャート

【図２４】受信契約関連情報に対する処理手順の一例を示すフローチャート

【図２５】コンテンツ利用条件の他の表現形式を示す図

【図２６】利用条件判定／修正部における処理手順の他の例を示すフローチャート

【図２７】有効期限に対する基本評価値の一例を示す図

【図２８】回数制限に対する基本評価値の一例を示す図

【図２９】機器限定に対する基本評価値の一例を示す図

【図３０】利用可能契約情報リストの他の例を示す図

【図３１】利用可能契約情報選択画面の一例を示す図

【図３２】利用条件判定／修正部における処理手順のさらに他の例を示すフローチャート

【図３３】２次利用出力部の内部構成の他の例を示す図

【図３４】２次利用出力部における処理手順の一例を示すフローチャート

【図３５】コンテンツ出力制御部の内部構成の一例を示す図

【図３６】コンテンツ出力制御部における処理手順の一例を示すフローチャート

【図３７】同実施形態に係る放送受信装置の他の構成例を示す図

【図３８】チャネル送信契約情報を含む電子番組ガイド情報の構造例を示す図

【図３９】放送コンテンツの暗号化機構について説明するための図

【図４０】放送コンテンツパケットの他のデータ構造を示す図

【図４１】受信契約関連情報パケットの他のデータ構造例を示す図

【図４２】契約情報のデータ構造例を示す図

【図４３】同実施形態に係る放送受信装置のさらに他の構成例を示す図

【図４４】同実施形態に係る放送受信装置における放送受信からパケットの内容に応じた処理までの全体的な処理手順の一例を示すフローチャート

【図４５】放送コンテンツパケットに対する処理手順の一例を示すフローチャート

【図４６】受信契約関連情報に対する処理手順の一例を示すフローチャート

【符号の説明】

１０１…受信部

１０２…Ａ／Ｄ変換部

１０３…誤り検出／訂正部

１０４…チャネル選択部

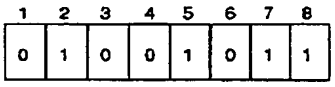
41

１０５…チャネル選択インタフェース
１０６…限定受信処理部（限定受信チップ）
１０７…コンテンツ利用法選択インタフェース
１０８…コンテンツ利用条件表示部
１１１…フィルター部
１１２…デスクランブル部
１１３…番組関連情報復号部
１１４…受信契約関連情報認証部
１１５…受信契約関連情報復号部
１１６…受信契約判定部
１１７…利用条件判定／修正部
１１８…コンテンツ出力制御部
１１９…チャネル情報入力部
１２０…標準出力部
１２１…２次利用出力部
１２２…マスター鍵格納部
１２３…受信装置ＩＤ格納部
１２４…ワーク鍵格納部
１２５…チャネルキー格納部

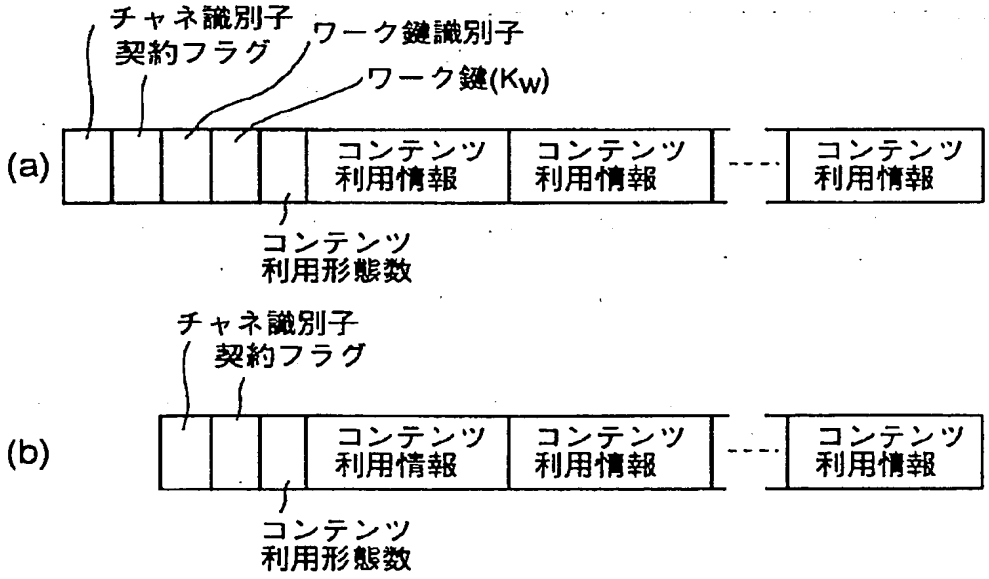
42

１２６…チャネルキー出力部
１２７…受信契約情報格納部
１２８…送信契約情報格納部
１２９…送信契約情報抽出部
２０１，２２１…コンテンツ入力部
２０２，２２３…コンテンツ暗号化部
２０３，２２４…コンテンツ出力部
２０４…コンテンツキー生成部
２０５，２２６，３０１…利用条件入力部
２０６，２２７…利用条件生成部
２０７…コンテンツＩＤ生成部
２０８…ライセンス情報生成部
２０９，２２５…機器マスター鍵格納部
２１０…ライセンス情報出力部
２２２…電子透かし埋め込み部
３０２…出力判定部
３０３…機器認証部
３０４…利用情報出力部

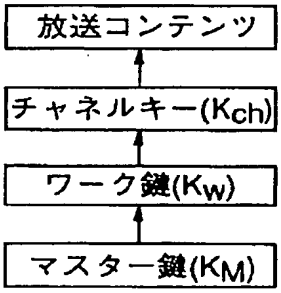
【図２】



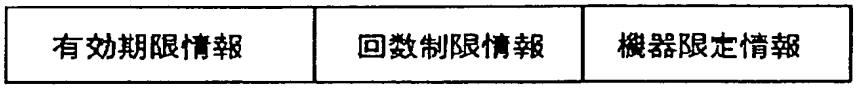
【図３】



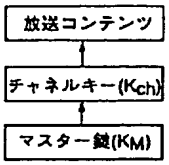
【図５】



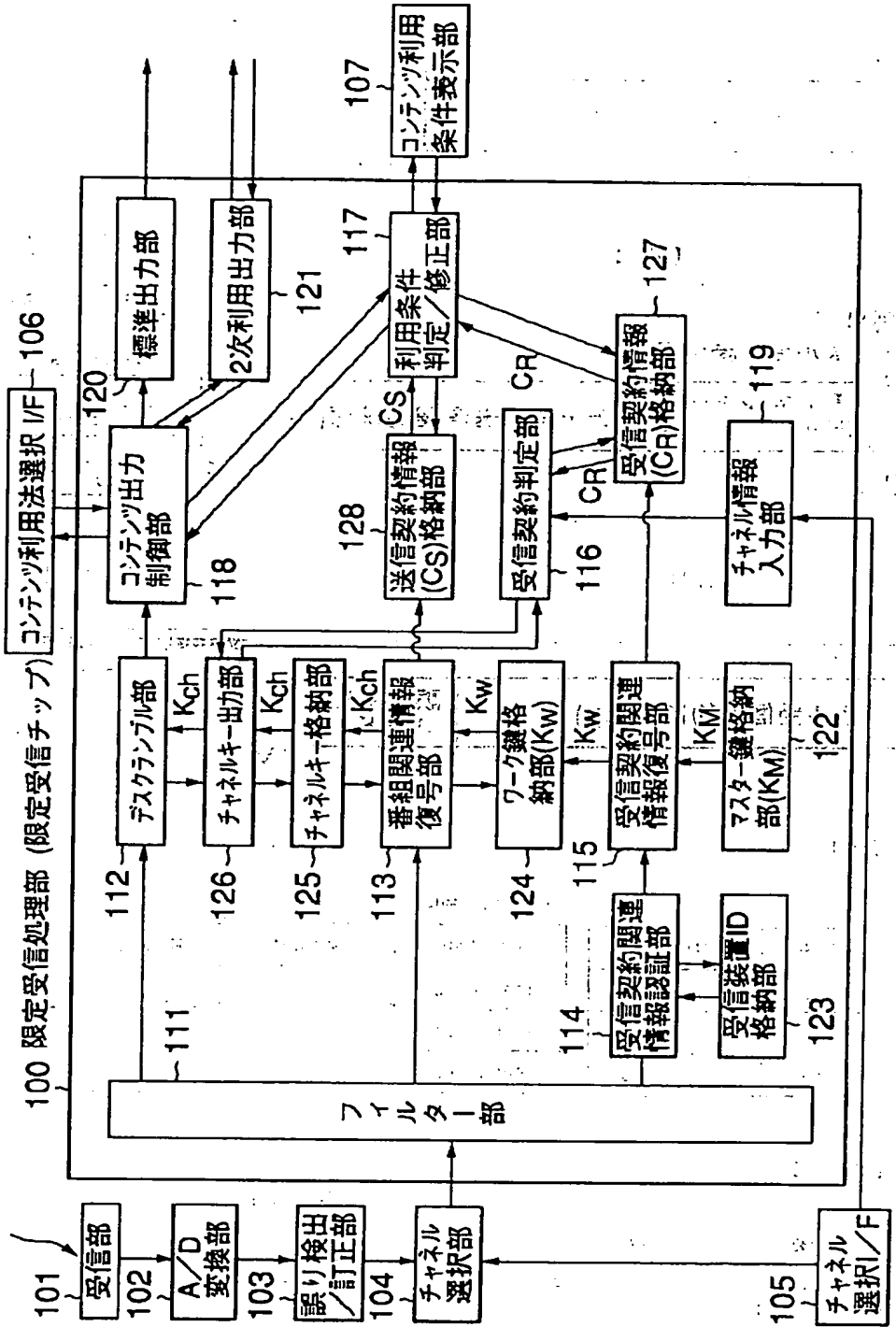
【図４】



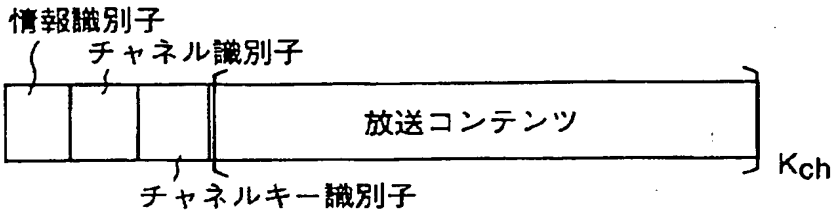
【図３９】



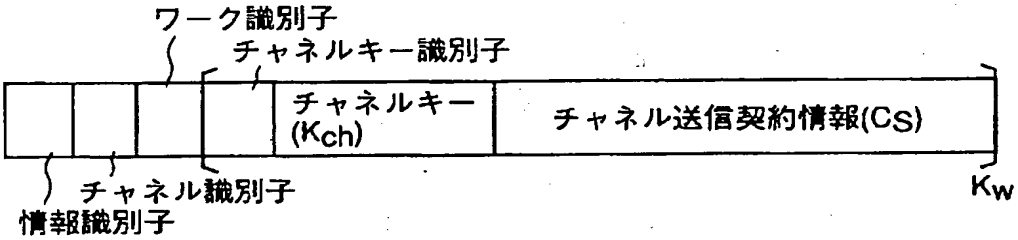
【図１】


100 限定受信処理部（限定受信チップ）
101 受信部
102 A/D変換部
103 誤り検出/訂正部
104 チャネル選択部
105 チャネル選択I/F
106 コンテンツ利用法選択 I/F
107 コンテンツ利用条件表示部
111 フィルター部
112 デスクランブル部
113 番組関連情報復号部
114 受信契約関連情報認証部
115 受信契約関連情報復号部
116 受信契約判定部
117 利用条件判定/修正部
118 コンテンツ出力制御部
119 チャネル情報入力部
120 標準出力部
121 2次利用出力部
122 マスター鍵格納部(KM)
123 受信装置ID格納部
124 ワーク鍵格納部(Kw)
125 チャネルキー格納部
126 チャネルキー出力部
127 受信契約情報(CR)格納部
128 送信契約情報(CS)格納部
Kch
Kw
KM
CS
CR

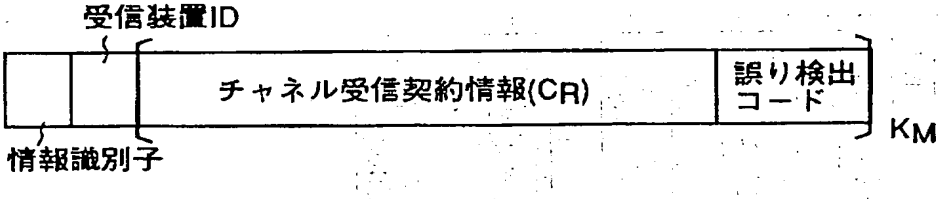
【図６】



【図７】

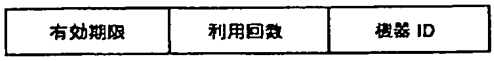


【図８】

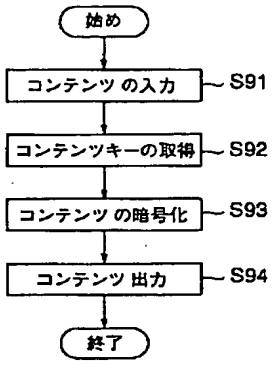


【図１３】

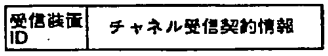
【図１８】



【図２２】



【図４２】



【図１４】

チャネル受信契約情報

有効期限情報	回数制限情報	機器限定情報
1999.06.10	-1	0
-1	3	1
2000.01.07	10	0

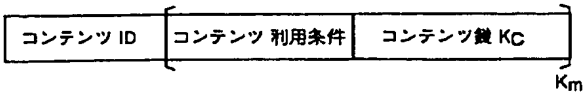
チャネル送信契約情報

有効期限情報	回数制限情報	機器限定情報
1999.05.20	-1	0
1999.07.31	-1	1
2000.01.07	15	1
-1	3	0

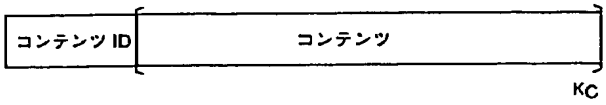
【図１６】

有効期限情報	回数制限情報	機器限定情報
1999.05.20	-1	0
1999.08.10	-1	1

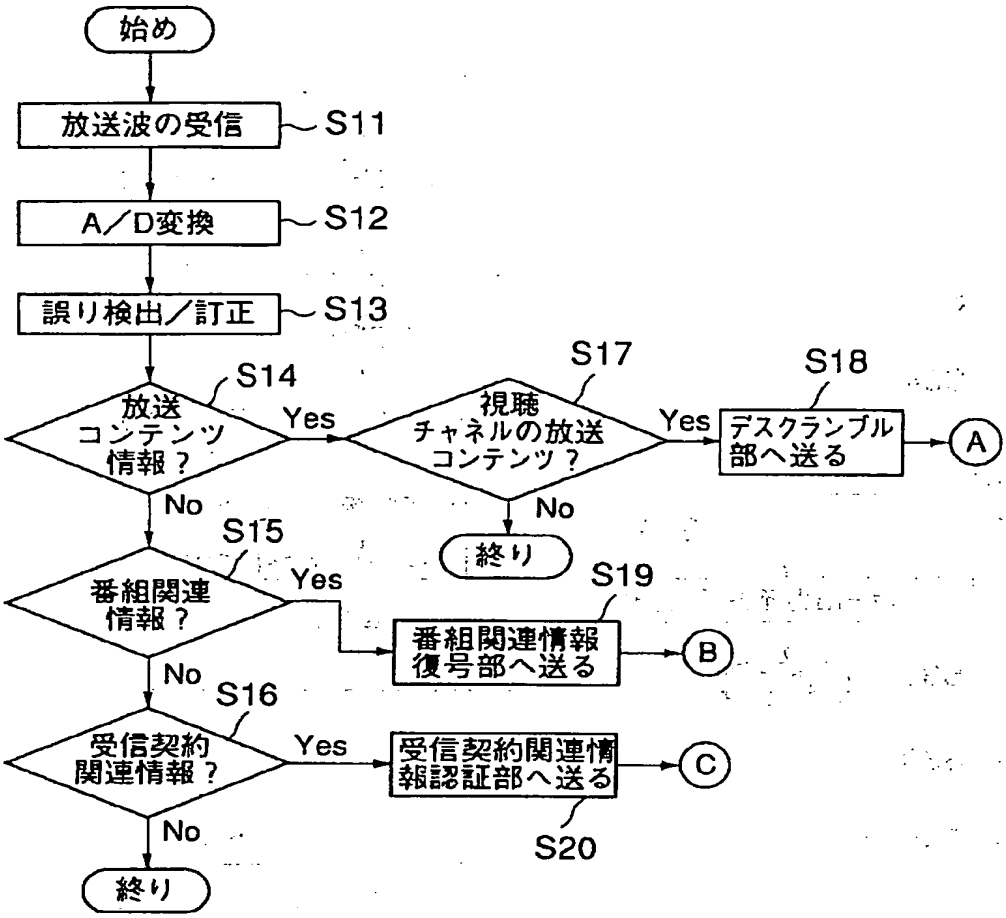
【図１７】



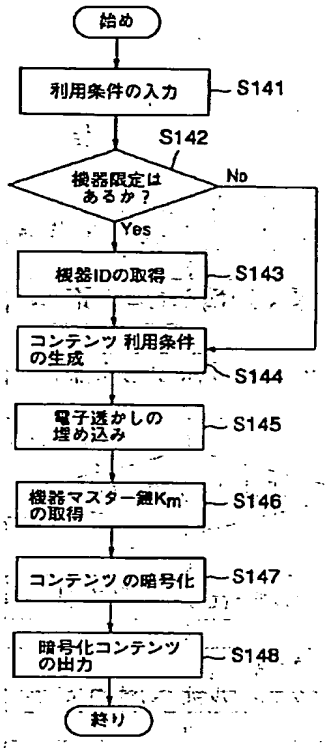
【図１９】



【図９】



【図３４】

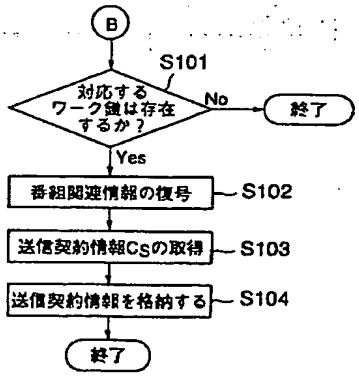


【図１５】

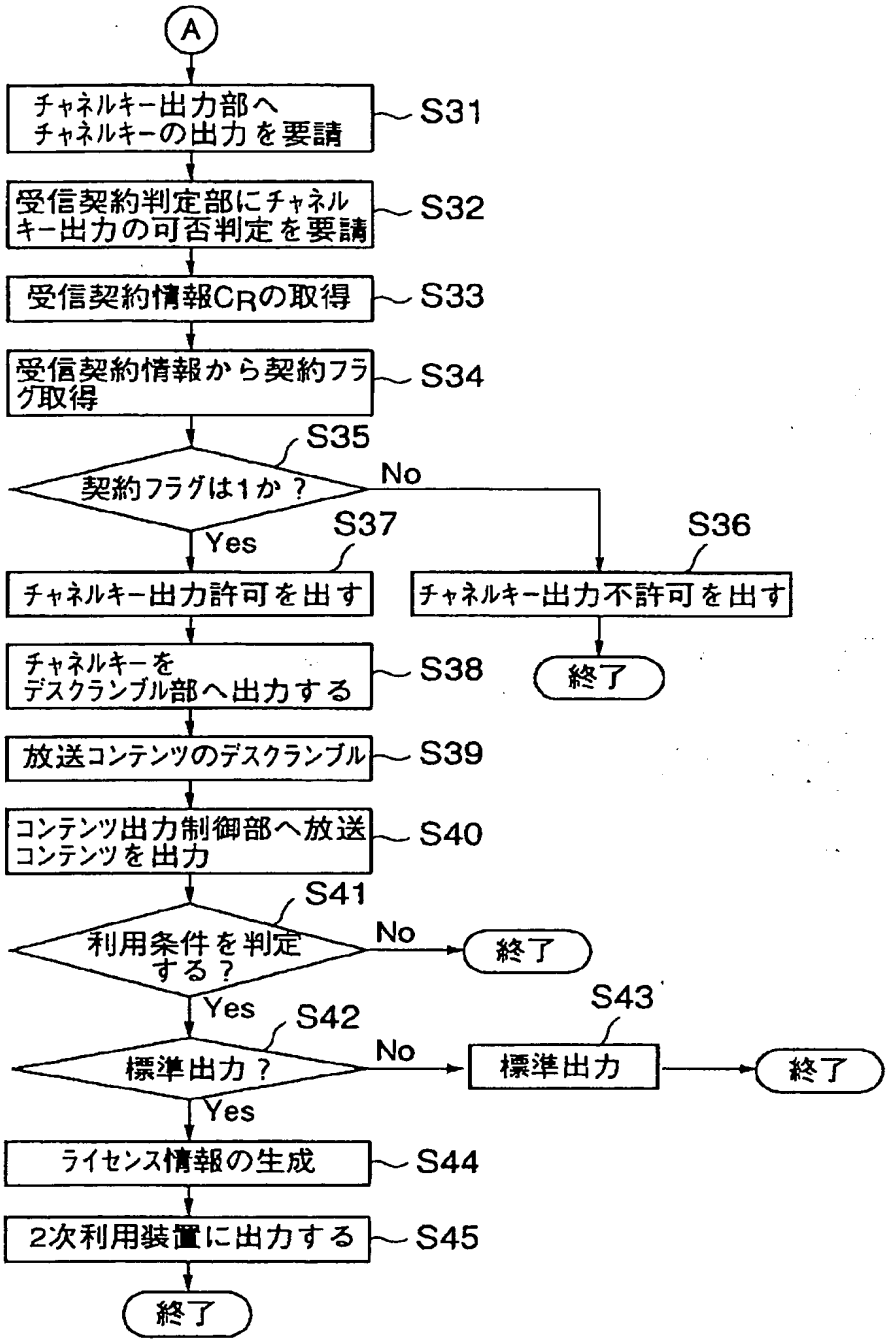
利用可能契約情報リスト

有効期限情報	回数制限情報	機器限定情報
1999.05.20	-1	0
1999.06.10	-1	1
1999.06.10	15	1
1999.06.10	3	0
1999.05.20	3	1
1999.07.31	3	1
2000.01.07	3	1
-1	3	1
1999.05.20	10	0
1999.07.31	10	1
2000.01.07	10	1
2000.01.07	3	0

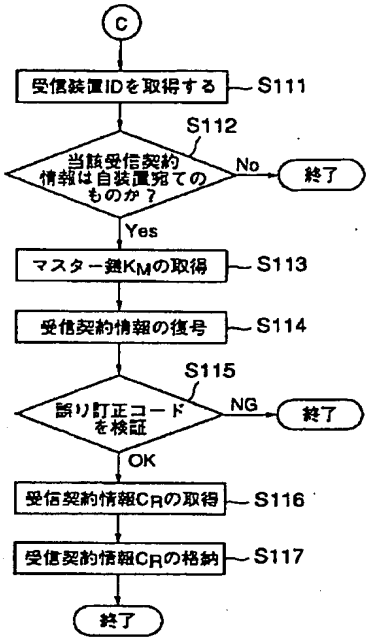
【図２３】



【図１０】



【図２４】



【図２７】

有効期限の基本評価値

有効期限との差	評価値
なし	10
3日以内	7
10日以内	3
それ以外	0

【図２８】

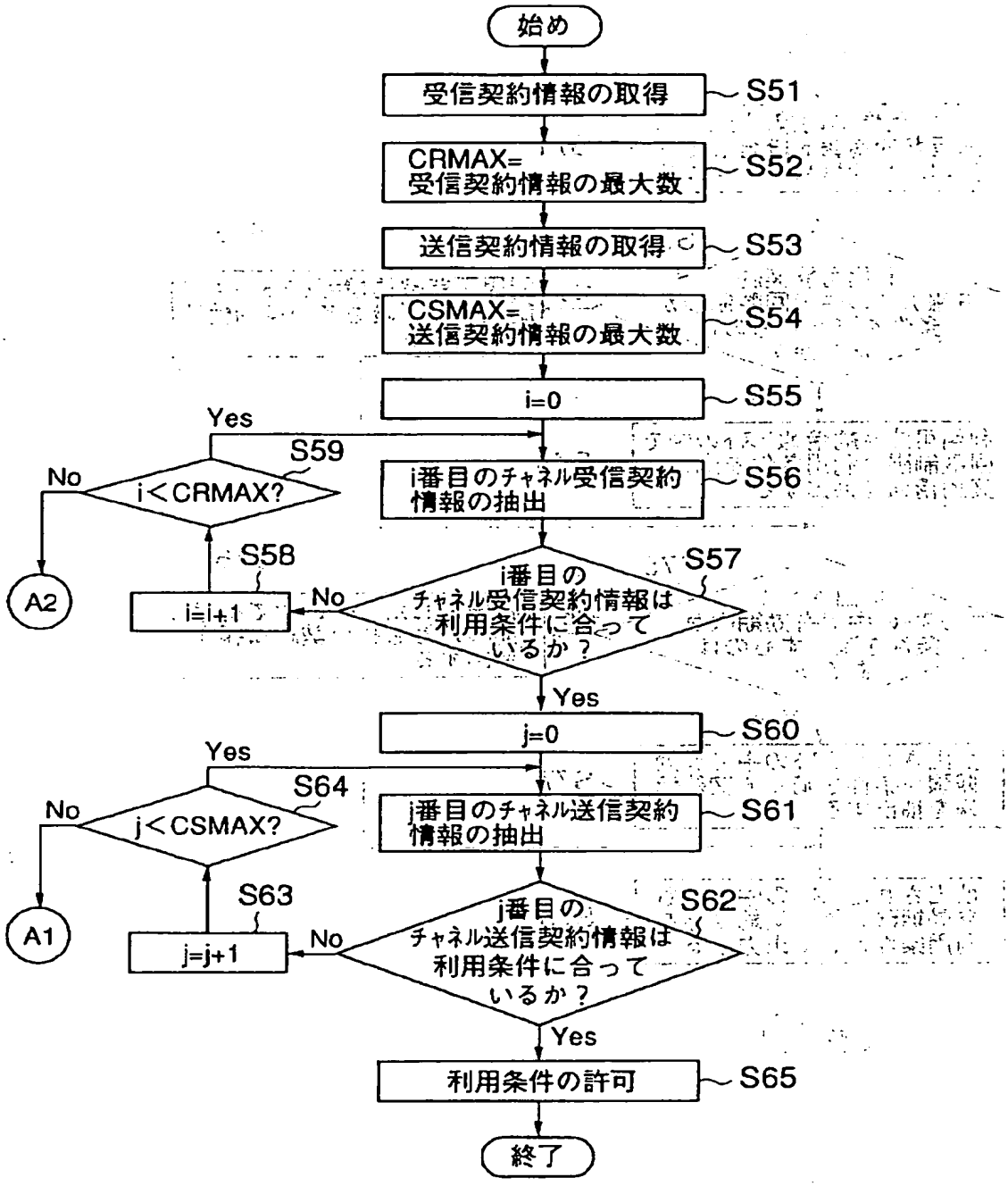
回数制限の基本評価値

回数制限との差	評価値
なし	10
3回以内	4
10回以内	1
11回以上	0

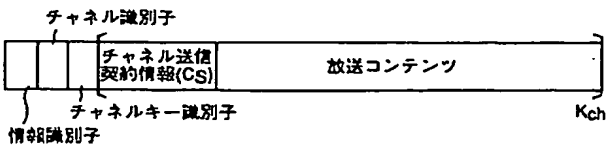
【図３８】

情報識別子	チャネル識別子	コンテンツ識別子	チャネル送信契約情報 (Cs)	番組情報

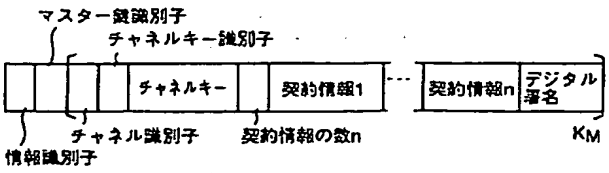
【図１１】


始め
受信契約情報の取得
S51
CRMAX=
受信契約情報の最大数
S52
送信契約情報の取得
S53
CSMAX=
送信契約情報の最大数
S54
i=0
S55
Yes
S59
No
i＜CRMAX?
i番目のチャネル受信契約情報の抽出
S56
S58
S57
A2
i=i+1
No
i番目のチャネル受信契約情報は利用条件に合っているか？
Yes
j=0
S60
Yes
S64
No
j＜CSMAX?
j番目のチャネル送信契約情報の抽出
S61
S63
S62
A1
j=j+1
No
j番目のチャネル送信契約情報は利用条件に合っているか？
Yes
利用条件の許可
S65
終了

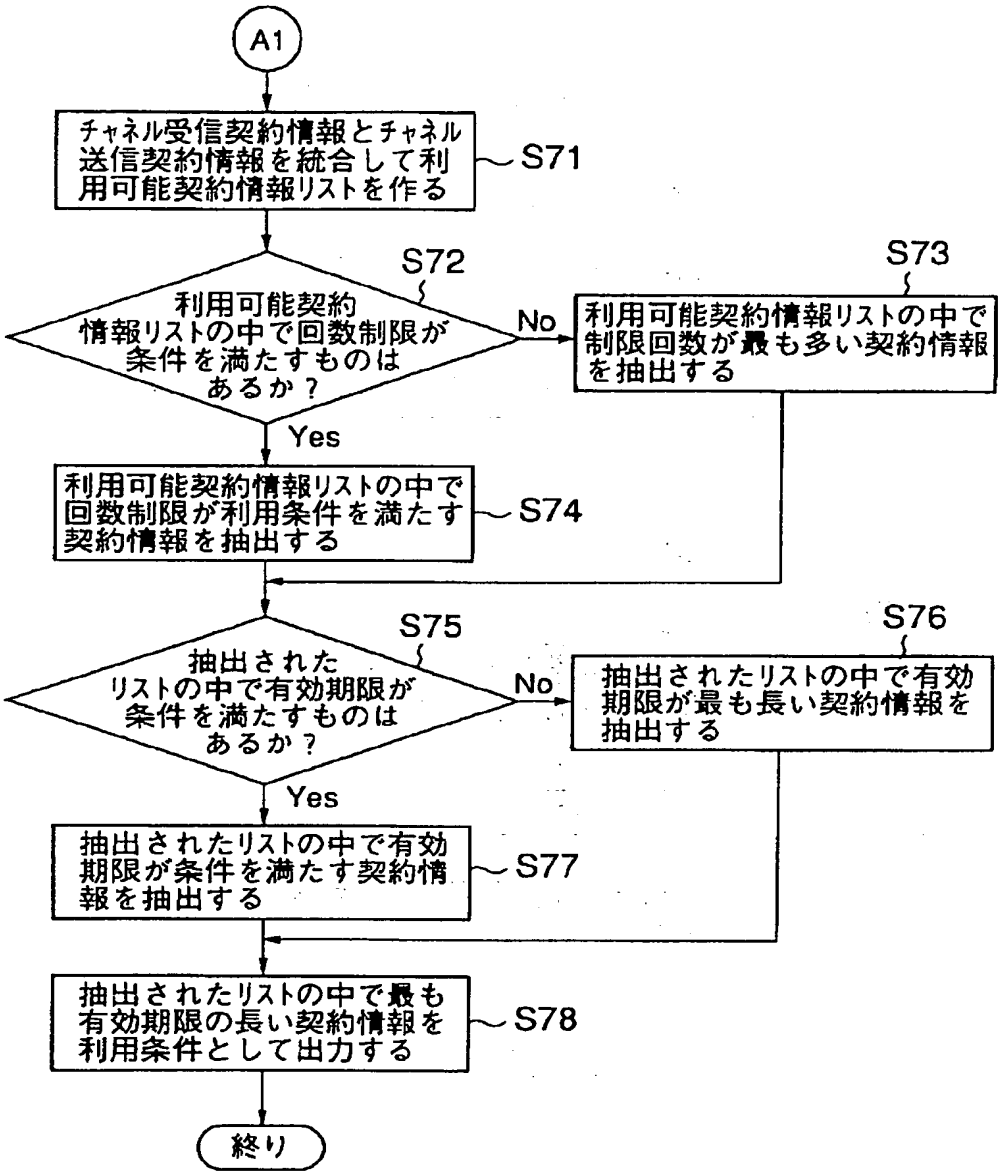
【図４０】


チャネル識別子
チャネル送信契約情報(Cs)
放送コンテンツ
チャネルキー識別子
情報識別子
Kch

【図４１】


マスター鍵識別子
チャネルキー識別子
チャネルキー
契約情報1
契約情報n
デジタル署名
チャネル識別子
契約情報の数n
情報識別子
KM

【図１２】

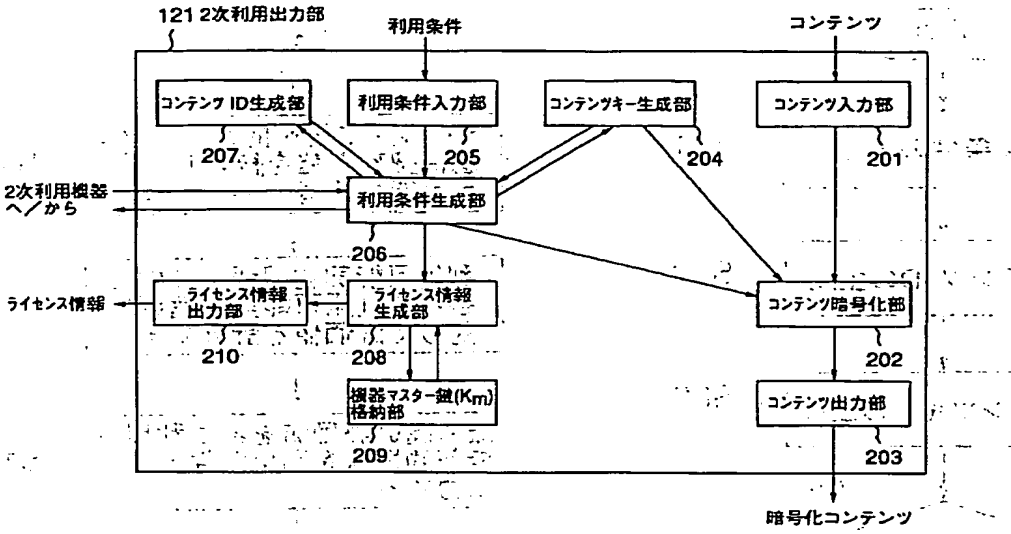


【図２９】

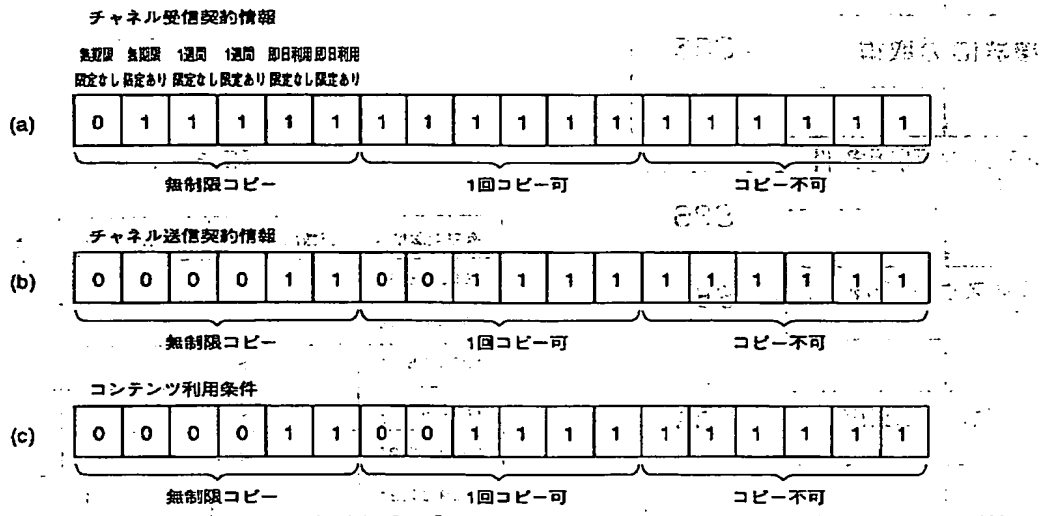
機器限定の基本評価値

利用条件の機器限定	希望条件の機器限定	評価値
1	1	10
1	0	0
0	1	10
0	0	10

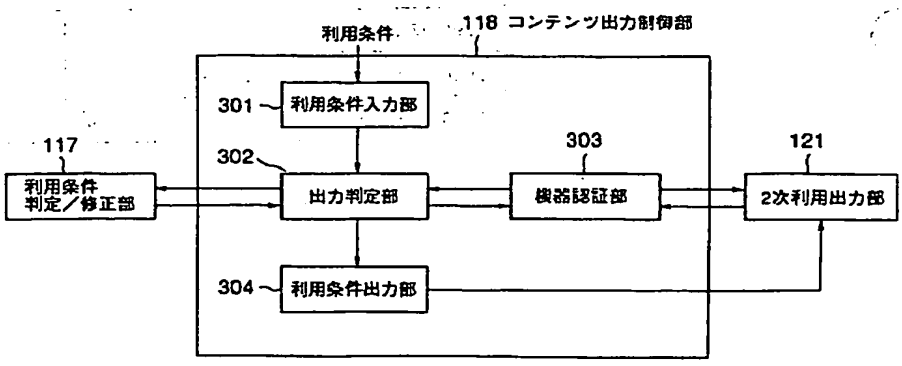
【図２０】


121 2次利用出力部
利用条件
コンテンツ
コンテンツ ID生成部
利用条件入力部
コンテンツキー生成部
コンテンツ入力部
207
205
204
201
2次利用機器へ／から
利用条件生成部
206
ライセンス情報
ライセンス情報出力部
ライセンス情報生成部
コンテンツ暗号化部
210
208
202
機器マスター鍵(Km)格納部
コンテンツ出力部
209
203
暗号化コンテンツ

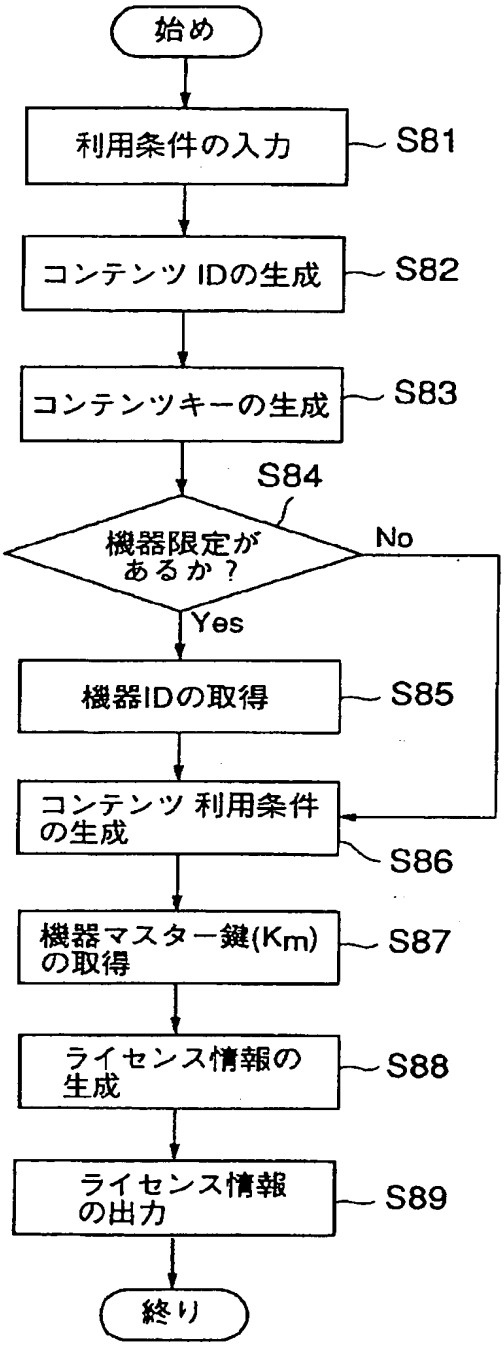
【図２５】


チャネル受信契約情報
無制限 無制限 1週間 1週間 即日利用 即日利用
限定なし 限定あり 限定なし 限定あり 限定なし 限定あり
(a)
0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
無制限コピー
1回コピー可
コピー不可
チャネル送信契約情報
(b)
0 0 0 0 1 1 0 0 1 1 1 1 1 1 1 1 1 1
無制限コピー
1回コピー可
コピー不可
コンテンツ利用条件
(c)
0 0 0 0 1 1 0 0 1 1 1 1 1 1 1 1 1 1
無制限コピー
1回コピー可
コピー不可

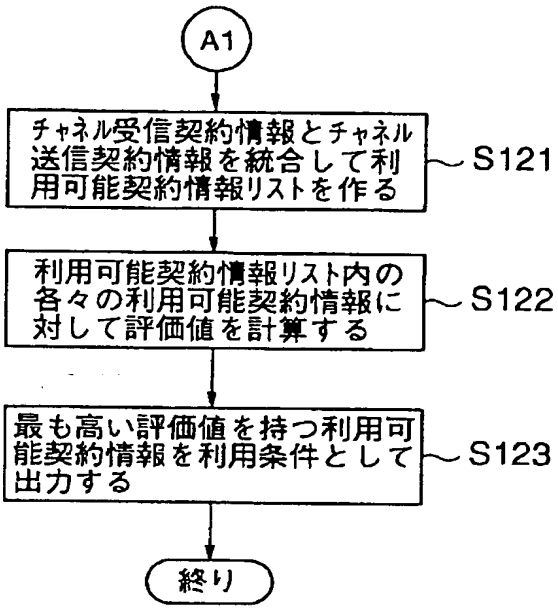
【図３５】


利用条件
118 コンテンツ出力制御部
301
利用条件入力部
117
302
303
121
利用条件判定／修正部
出力判定部
機器認証部
2次利用出力部
304
利用条件出力部

【図２１】



【図２６】



【図３０】

有効期限情報	回数制限情報	機器限定情報	評価値
1999.05.20	-1	0	70
1999.06.10	-1	1	50
1999.06.10	15	1	50
1999.06.10	3	0	40
1999.05.20	3	1	20
1999.07.31	3	1	20
2000.01.07	3	1	120
-1	3	1	120
1999.05.20	10	0	70
1999.07.31	10	1	50
2000.01.07	10	1	150
2000.01.07	3	0	140

【図３１】

利用可能契約情報選択画面

可能な利用形態は以下のものです。コンテンツの利用形態を選択して下さい。

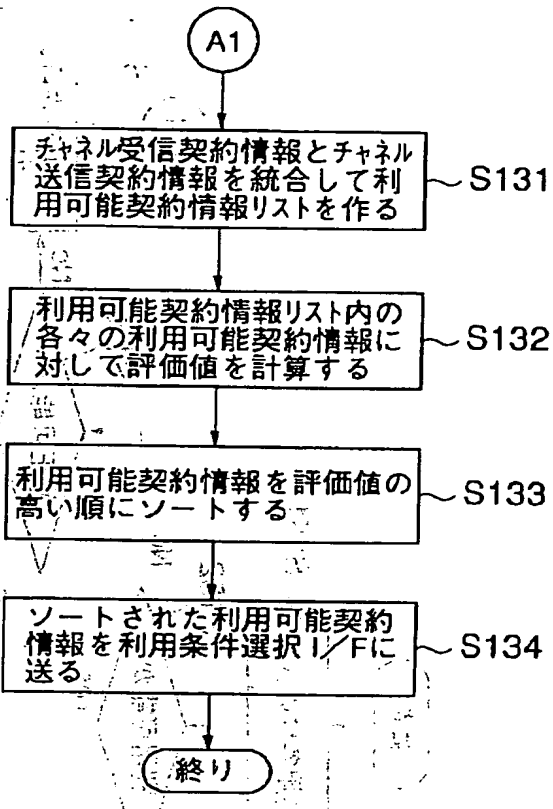
コンテンツ名　ブラームス　交響曲1番

利用可能形態

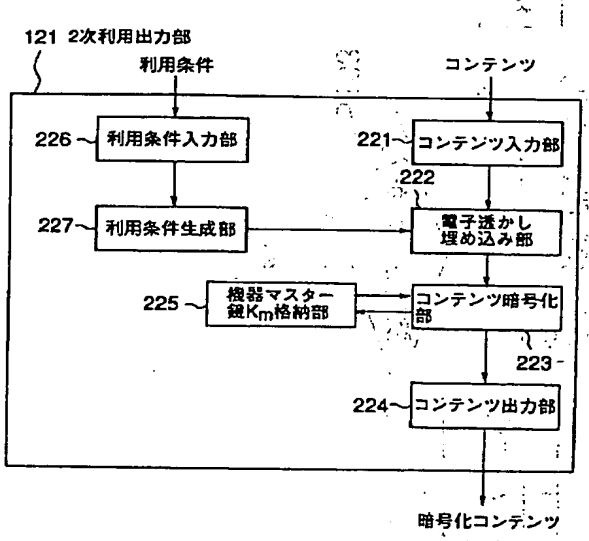
	有効期限	回数制限	機器限定
①	2000.01.07	10	あり
②	2000.01.07	3	なし
③	無期限	3	あり
④	2000.01.07	3	あり
⑤	1999.05.20	なし	なし

次の5件

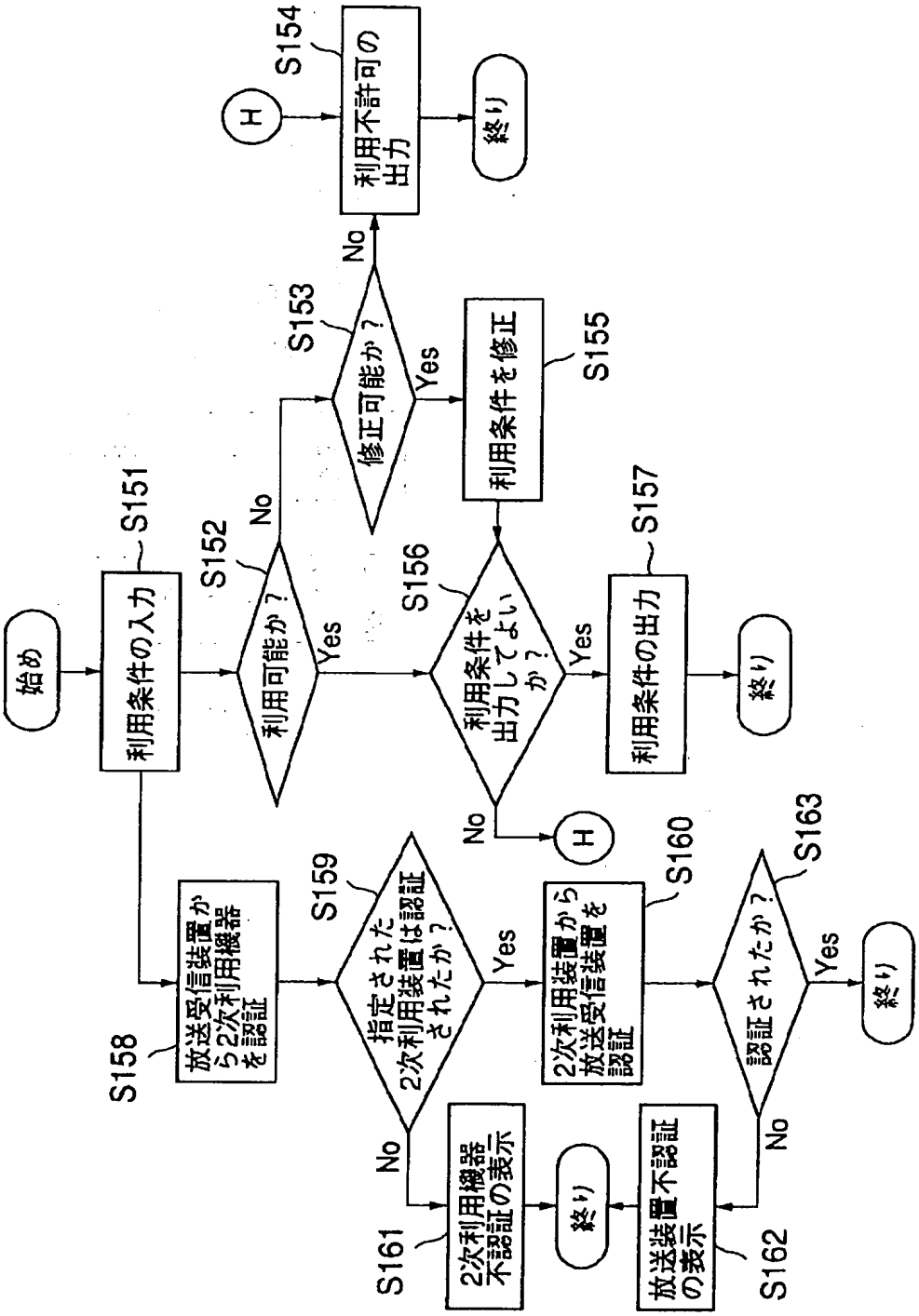
【図３２】



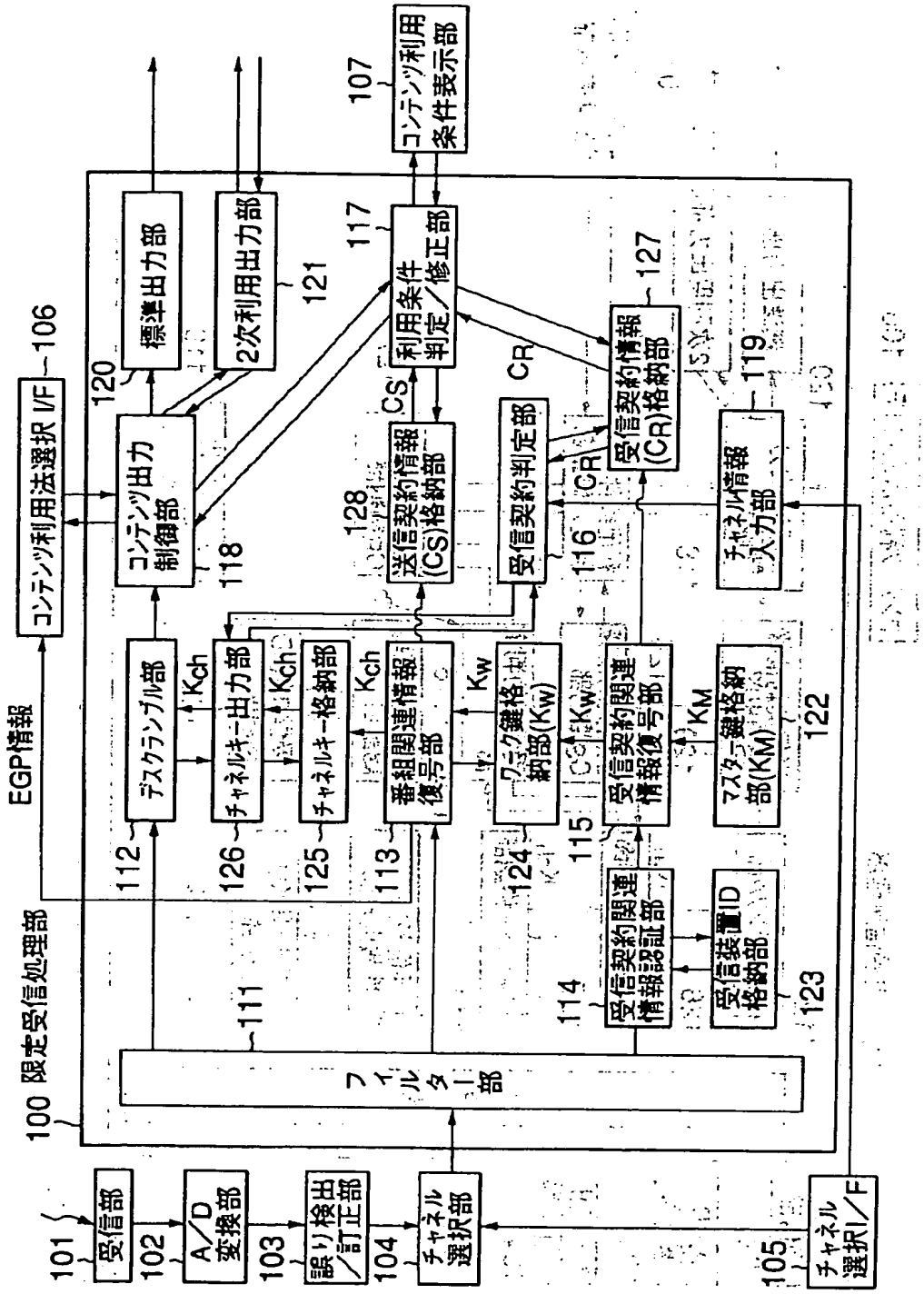
【図３３】



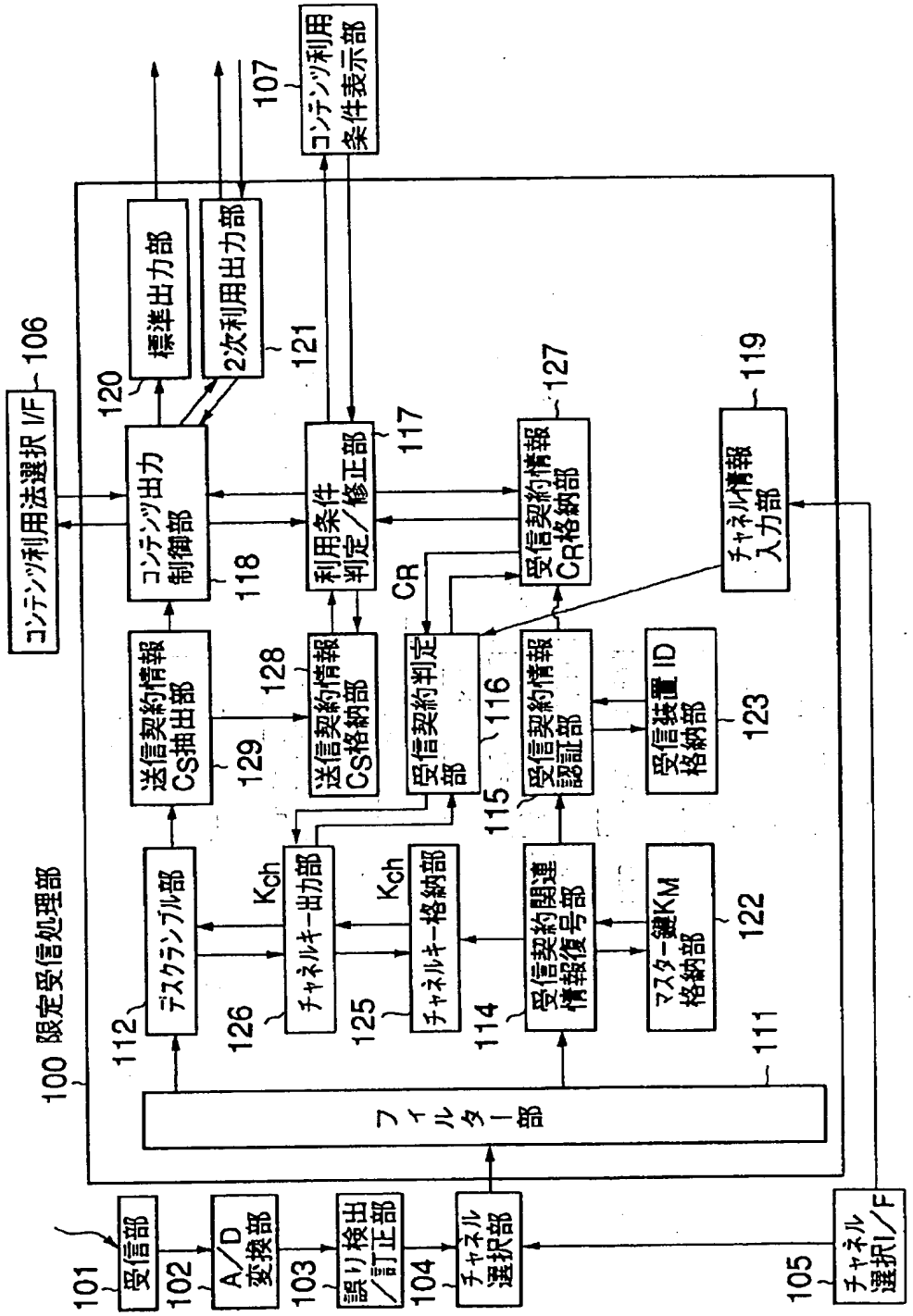
【図３６】


始め
利用条件の入力
S151
利用可能か？
S152
No
Yes
修正可能か？
S153
No
Yes
利用不許可の出力
S154
終り
利用条件を修正
S155
利用条件を出力してよいか？
S156
Yes
No
利用条件の出力
S157
終り
H
H
放送受信装置から2次利用機器を認証
S158
指定された2次利用装置は認証されたか？
S159
No
Yes
2次利用機器不認証の表示
S161
終り
2次利用装置から放送受信装置を認証
S160
認証されたか？
S163
No
Yes
放送装置不認証の表示
S162
終り

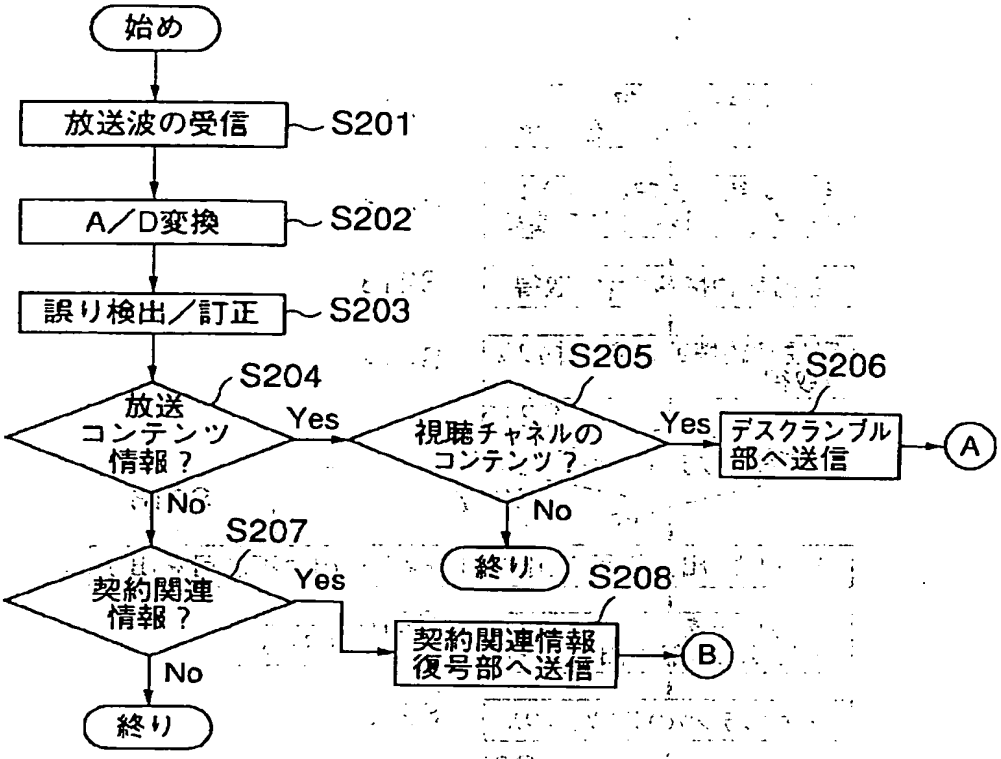
【図３７】


100 限定受信処理部
101 受信部
102 A/D変換部
103 誤り検出/訂正部
104 チャネル選択部
105 チャネル選択I/F
106 コンテンツ利用法選択 I/F
107 コンテンツ利用条件表示部
111 フィルター部
112 デスクランブル部
113 番組関連情報復号部
114 受信契約関連情報認証部
115 受信契約関連情報復号部
116 受信契約判定部
117 利用条件判定/修正部
118 コンテンツ出力制御部
119 チャネル情報入力部
120 標準出力部
121 2次利用出力部
122 マスター鍵格納部(KM)
123 受信装置ID格納部
124 ワーク鍵格納部(Kw)
125 チャネルキー格納部
126 チャネルキー出力部
127 受信契約情報(CR)格納部
128 送信契約情報(CS)格納部
EGP情報
Kch
Kw
KM
CS
CR

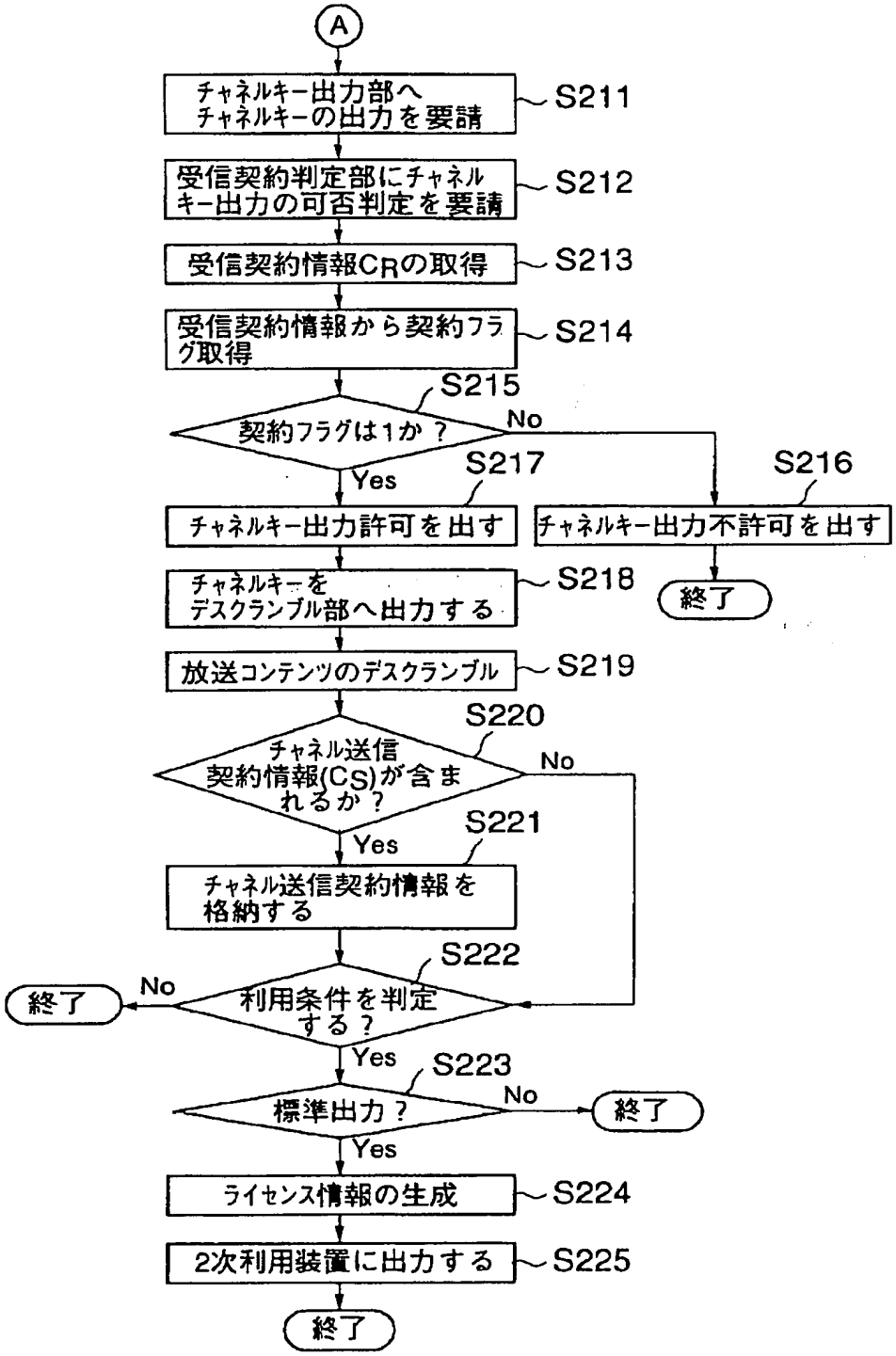
【図４３】


100 限定受信処理部
101 受信部
102 A/D変換部
103 誤り検出/訂正部
104 チャネル選択部
105 チャネル選択I/F
106 コンテンツ利用法選択 I/F
107 コンテンツ利用条件表示部
111 フィルター部
112 デスクランブル部
114 受信契約関連情報復号部
115 受信契約認証部
116 受信契約判定部
117 利用条件判定/修正部
118 コンテンツ出力制御部
119 チャネル情報入力部
120 標準出力部
121 2次利用出力部
122 マスター鍵KM格納部
123 受信装置ID格納部
125 チャネルキー格納部
126 チャネルキー出力部
127 受信契約情報CR格納部
128 送信契約情報CS格納部
129 送信契約情報CS抽出部
Kch
Kch
CR

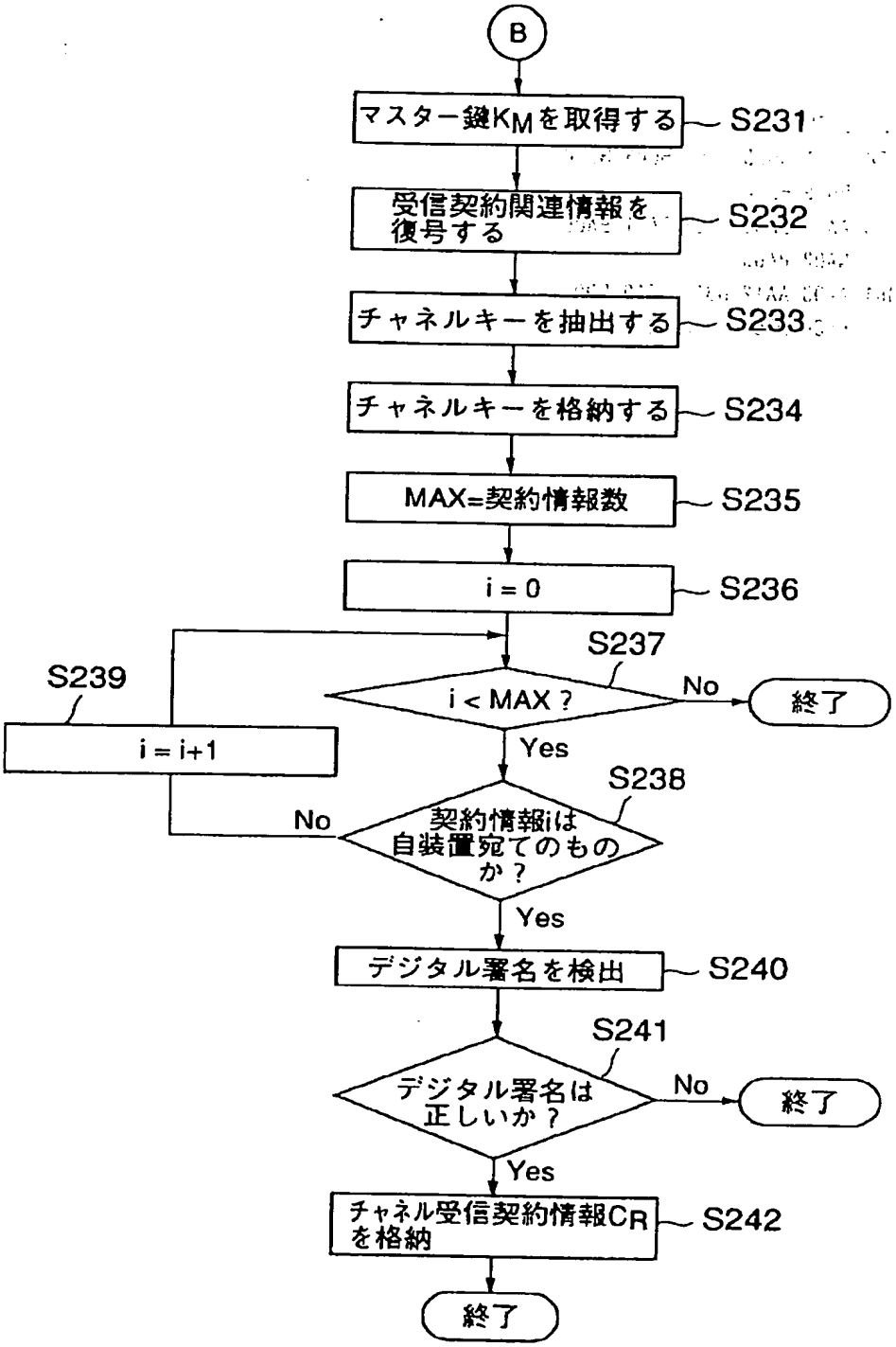
【図４４】


始め
放送波の受信
S201
A／D変換
S202
誤り検出／訂正
S203
S204
放送コンテンツ情報？
Yes
No
S205
視聴チャネルのコンテンツ？
Yes
No
S206
デスクランブル部へ送信
A
終り
S207
契約関連情報？
Yes
No
S208
契約関連情報復号部へ送信
B
終り

【図４５】


A
チャネルキー出力部へチャネルキーの出力を要請
S211
受信契約判定部にチャネルキー出力の可否判定を要請
S212
受信契約情報CRの取得
S213
受信契約情報から契約フラグ取得
S214
S215
契約フラグは1か？
No
Yes
S217
S216
チャネルキー出力許可を出す
チャネルキー出力不許可を出す
終了
チャネルキーをデスクランブル部へ出力する
S218
放送コンテンツのデスクランブル
S219
S220
チャネル送信契約情報(CS)が含まれるか？
No
Yes
S221
チャネル送信契約情報を格納する
S222
終了
No
利用条件を判定する？
Yes
S223
標準出力？
No
終了
Yes
ライセンス情報の生成
S224
2次利用装置に出力する
S225
終了

【図４６】


B
マスター鍵K_Mを取得する
S231
受信契約関連情報を復号する
S232
チャネルキーを抽出する
S233
チャネルキーを格納する
S234
MAX=契約情報数
S235
i = 0
S236
S237
i < MAX ?
No
終了
Yes
S239
i = i+1
S238
No
契約情報iは自装置宛てのものか？
Yes
デジタル署名を検出
S240
S241
デジタル署名は正しいか？
No
終了
Yes
チャネル受信契約情報CRを格納
S242
終了

フロントページの続き

(51) Int. Cl.⁷	識別記号	Ｆ Ｉ		ﾃｰﾏｺｰﾄﾞ (参考)
Ｈ０４Ｎ　7/16		Ｈ０４Ｌ	9/00	６０１Ｅ
				６８５

Ｆターム (参考)　5C025 CB08 DA01 DA05
5C064 BA01 BB05 BB07 BC06 BC20
BD09 BD14
5J104 AA01 BA03 DA03 EA01 EA06
NA02 PA05
5K061 AA00 AA12 BB17 BB19 DD00
FF00 FF01 JJ03 JJ07